der Bundeswehr
Universität München

Masterarbeit

Aufbau einer Quantenkommunikationsinfrastruktur - Test und Parameterstudien von Quantenkommunikationsgeräten

Eingereicht von: Paul Meik Kalwa
1173229

Erstprüfung: Prof. Dr. Udo Helmbrecht
Zweitprüfung: Prof. K. Buchenrieder, Ph.D.

Betreuer: Dr. Matthias Lienert

Abgabedatum: 30. Juni 2021

Universität der Bundeswehr München
Forschungsinstitut CODE

Inhaltsverzeichnis

Kapitel 1

Einleitung und Problemstellung

1.1 Einleitung

Durch das Voranschreiten der digitalen „Welt“ nimmt die Digitalisierung im Allgemeinen sowie auch die Kommunikation im digitalen Raum einen immer größer werdenen Platz in der Gesellschaft ein. Dazu gehört ein großes Spektrum an Dienstleistungen, wie zum Beispiel das Onlinebanking, das Onlineshopping oder die Onlinekommunikation allgemein. Dieses bietet zwar viele Erneuerungen zur Vereinfachung des Alltags, aber gleichzeitig bringt es auch viele neue Angriffsmöglichkeiten mit sich. Aus diesem Grund ist die Kryptographie, beziehungsweise die Verschlüsselung aller sensiblen Daten, ein wichtiges Thema.
Auch in dem militärischen Kontext spielt die Verschlüsselung eine wichtige Rolle. So dürfen Waffensysteme und militärisch relevante Satelliten auf keinen Fall von nicht autorisierten Personen oder Personengruppen gehackt beziehungsweise unter Kontrolle gebracht werden.
Neue Ansätze der Kryptographie sind die Quantenkryptographie, insbesondere der Quantenschlüsselaustausch (englisch „Quantum key distribution (QKD))“ und die „Post-Quantum-Kryptographie“. Diese Ansätze werden aufgrund der schnellen Entwicklung von Quantencomputern verfolgt. Quantencomputer sind in vermutlich circa 10 Jahren auf einem Entwicklungsstand, der es ermöglicht, viele der aktuellen asymmetrischen Verschlüsselungsverfahren zu brechen. Aufgrund der Möglichkeit, sensible Daten abzuhören und deren Verschlüsselung zu einem späteren Zeitpunkt zu knacken, ist es von Nöten, auf eine sichere Verschlüsselungsalternative auszuweichen. Die „Post-Quantum-Kryptographie“ ist ein Sammelbegriff für (klassische) mathematische Verschlüsselungsalgorithmen, basierend auf Problem, die nach aktuellem Kenntnisstand nicht von Quantencomputern zu brechen sind. Der Quantenschlüsselaustausch generiert einen sicheren Schlüssel, basierend auf den Prinzipien der Quantenphysik.
Durch den Quantenschlüsselaustausch kann eine beliebig lange Zufallszahl erstellt werden, auf die zwei oder mehrere Parteien zugreifen können. Diese Zufallszahl kann nach dem Erstellen von symmetrischen Verschlüsselungsverfahren beziehungsweise von Programmen zur Verschlüsselung von Daten genutzt werden. Ein Vorteil des Quantenschlüsselaustausches ist es, dass dieser abhörsicher ist, da man das Abhören einer uner-

wünschten Partei mitbekommt. Ist dies der Fall, kann einfach eine neue Zufallszahl generiert werden. Um den Quantenschlüsselaustausch durchzuführen und eine Zufallszahl zu generieren, werden Quantenschlüsselverteilungsplattformen benötigt. Dieses Thema wird in Kapitel 2 näher erläutert.
Diese Arbeit beschäftigt sich mit der Untersuchung verschiedenster Einflüsse und deren Auswirkungen auf die Quantenschlüsselverteilungsplattform Clavis[3], von dem Hersteller ID Quantique, welche in dem Projekt MuQuaNet eingesetzt werden soll.
Dazu wird zu Anfang kurz auf den theoretischen Hintergrund des Quantenschlüsselaustausches, mit Augenmerk auf das BB84-Protokoll und das Coherent One-Way-Protokoll, eingegangen. Danach folgt eine Vorstellung der Quantenschlüsselverteilungsplattform, welche im Zuge des Projekts MuQuaNet eingesetzt werden soll und des Versuchsaufbaus. Dabei werden auch die mitgelieferte Software und die dazugehörigen Werte erklärt. Daraufhin werden die verschiedenen Messreihen erklärt und mit Hilfe von Diagrammen ausgewertet. Auch werden dazu die verschiedenen Forschungsfragen behandelt. Den Abschluss der Arbeit bildet das letzte Kapitel, in dem die Arbeit zusammengefasst und ein Ausblick gegeben wird.

1.2 Problemstellung

Die Nutzung und das Verhalten der Quantenschlüsselverteilungsplattform Clavis[3] wirft in Bezug auf verschiedene Aspekte noch verschiedene Fragen auf. Aus diesem Grund ist es Ziel dieser Arbeit, die Quantenschlüsselverteilungsplattform in Bezug auf das Projekt zu untersuchen.
Dazu stellt sich die Forschungsfrage, wie sich die „Quantum Bit Error Rate“, die „Visibility“ und die „Secret Key Rate“ im Vergleich mit den vom Hersteller angegebenen Werten bei verschiedenen Studien verhalten. Hierbei geht es um die Stabilität der Geräte im Zeitverlauf, die Optimierung dieser durch Fehlerbeseitigungen und dem Vermeiden von auftretenden Störungen durch äußere Einflüsse. Hinzufügend soll herausgefunden werden, welches die optimale optische Dämpfung für die Stabilität der Geräte sowie für die Schlüsselgenerierung ist. Genauer:

- Wie stabil ist die Quantenschlüsselverteilungsplattform über einen längeren Zeitraum? Welche Besonderheiten beziehungsweise Störungen lassen sich beobachten?
- Wie lassen sich äußere Einflüsse vermeiden beziehungsweise vermindern, um einen Anstieg der „Visibility“ und eine Reduktion der „Qber“ zu bewirken?
- Wie verhalten sich die Geräte bei einem simulierten Angriff durch einen Eavesdropping-Simulator? Welche Auswirkungen hat ein solcher Angriff und wie lässt sich dieser erkennen?
- Bei welcher optischen Dämpfung wird die optimale Schlüsselrate sowie die bestmögliche Stabilität gewährleistet?

- Wie hoch ist die maximale optische Dämpfung, bei der noch ein stabiler Schlüsselaustausch möglich ist?

Des Weiteren gilt es, Erkenntnisse aus den Messungen zu ziehen und herauszufinden, welche Grundbedingungen bei dem Einsatz der Geräte, in Bezug auf das Projekt MuQuaNet, beachtet werden müssen. Die Definition der „Visibility“, der „Qber“ und der „Secret Key Rate“ finden sich am Ende des Unterkapitels 3.2.1.

Kapitel 2

Einführung: Quantenkryptographie

Das folgende Kapitel dient dem Einblick in die Quantenkryptographie und den Quantenschlüsselaustausch. Auch wird hier auf zwei verschiedene Protokolle des Quantenschlüsselaustausches eingegangen.

2.1 Quantenkryptographie

Im Gegensatz zu der klassischen Kryptographie benutzt die Quantenkryptographie quantenmechanische Effekte zur Verschlüsselung von Nachrichten. Bekannte Physiker, wie Werner Heisenberg, Max Born, Erwin Schrödinger und Pascual Jordan, befassten sich mit einer, in der Mitte der 1920er Jahre entwickelten, physikalischen Theorie der Quantenmechanik. Der Quantenschlüsselaustauch, welcher die Grundlage der Quantenkryptographie bildet, basiert auf dieser Theorie, mit deren Hilfe sich die Gesetzmäßigkeiten von Atomen und kleineren Teilchen besser als mit der klassischen Physik erklären lassen. [2]
Ein Vorteil der Quantenkryptographie ist, dass die Sicherheit hinter dem System auf physikalischen Eigenschaften basiert und nicht auf mathematischen Problemen. Eine quantenmechanische Messung beeinflusst das System grundsätzlich auf substanzielle Art und Weise. So lässt sich beispielsweise ein Abhörversuch bei dem Schlüsselaustausch erkennen, da der Angreifer auf eine solche Messung zurückgreifen muss. Wird ein Angriff erkannt, kann der Schlüssel gegebenenfalls ausgetauscht oder auf einer anderen Leitung neu verhandelt werden. [2]
Ende 2018 gelang es dem Wiener Team von dem Institut für Quantenoptik erstmals, mehr als zwei Teilnehmer per Quantenverschlüsselung online zu verbinden. Das österreichische Team schaltete eine Konferenz von 4 Teilnehmern. Nach Aussage des Forschungsteams ist es möglich, die Anzahl der Teilnehmer relativ einfach zu erweitern. Deswegen ist die Quantenkryptographie ein vielversprechendes Mittel, um Konferenzschaltungen abhörsicher zu machen. [2]

2.2 Quantenschlüsselaustausch

Mit Hilfe des Quantenschlüsselaustausches besteht die Möglichkeit, zwei oder mehreren Parteien eine gemeinsame Zufallszahl zur Verfügung zu stellen. Die erstellte gemeinsame Zufallszahl kann danach als geheimer Schlüssel zur Verschlüsselung von Nachrichten durch klassische symmetrische Kryptographie verwendet werden. Dazu zählen zum Beispiel die Verschlüsselungsverfahren „AES“ und „3DES“ sowie das „One-Time-Pad“, welches normalerweise mit hohen Kosten verbunden ist und deswegen nicht oft genutzt wird. Klassische und quantenmechanische Systeme können, trotz hoher Rechenleistung, die Sicherheit des Quantenschlüsselaustausches nicht überwinden, da diese auf Naturgesetzen basiert. [5] [3]
Für den Austausch von Quantenschlüsseln wird kein Quantencomputer benötigt. Es werden lediglich Quantenschlüsselverteilungsplattformen benötigt, die Quantenzustände, zum Beispiel durch polarisierte Photonen, übertragen. Die Quantenschlüsselverteilungsplattformen bestehen mindestens aus einem offenen oder durch ein Glasfaserkabel realisierten Quantenkanal, einem authentifizierten Kommunikationskanal zum Einrichten eines Quantenschlüssels und einem Austauschprotokoll, welches zum Quantenschlüsselaustausch verwendet wird, mit den zur Realisierung des Austauschprotokolls benötigten Komponenten. Die Distanz, über die ein Quantenschlüsselaustausch stattfinden kann, ist durch die moderne Fastertechnik begrenzt. Die technische Dämpfung von Glasfaserkabeln beträgt etwa 0,2 Dezibel pro Kilometer, sodass nach 50 Kilometern circa zehn Prozent und nach 100 Kilometern nur noch ein Prozent der ursprünglichen Intensität der Photonen vorhanden ist. [3] [5]
Aufgrund der physikalischen Gesetze, auf denen der Austausch von Quantenschlüsseln basiert, ist die Sicherheit nicht durch Annahmen über die Leistung von Computern und Algorithmen gewährleistet. Dies ist ein großer Vorteil gegenüber klassischen Methoden der Schlüsselverteilung. Ein weiterer Vorteil des Quantenschlüsselsaustauschs ist, dass der Versuch des Abhörens des Schlüssels bemerkt wird. Somit kann der abgehörte Schlüssel verworfen und ein neuer erzeugt werden. [3] [5]

2.2.1 BB84-Protokoll

Konventionellen Kryptosystemen liegt eine Mischung aus Vermutungen und Mathematik zu Grunde. Diese Kryptosysteme mit geheimen Schlüsseln können laut der Informationstheorie nur dann absolut sicher sein, wenn der Schlüssel mindestens so lang wie der Klartext ist und jeder Schlüssel nur einmal verwendet wird. Die heutzutage eingesetzten „Public-Key-Kryptosysteme“ sind nicht sicher gegen Angriffe von Quantencomputern. Zumal in der konventionellen Kryptographie davon ausgegangen wird, dass digitale Kommunikation immer passiv überwacht und kopiert werden kann, wird als möglicher Lösungsansatz die Unschärferelation der Quantenphysik genutzt. Auch ändert jede quantenmechanische Messung den Zustand eines Systems auf nicht zu minimierende Art und Weise. [5]
Wenn Informationen in nicht-orthogonalen Quantenzuständen, wie zum Beispiel mit Hilfe von einzelnen Photonen mit den Polarisationsrichtungen 0°, 90°, 45° und 135°,

kodiert werden, erhält man einen Kommunikationskanal, der nicht von einem Abhörer gelesen oder kopiert werden kann, ohne dass dieser gewisse Schlüsselinformationen kennt, die bei der Bildung der Übertragung verwendet wurden. Der Abhörer kann auch, ohne die Übertragung auf eine zufällige und unkontrollierbare Weise zu beeinflussen, keine Teilinformationen erlangen, da dies mit hoher Wahrscheinlichkeit von den Nutzern des Kanals entdeckt wird. [5]
Polarisiertes Licht wird erzeugt, indem ein gewöhnlicher Lichstrahl durch eine Polarisationsapparatur, wie beispielsweise einem Calcitkristall oder einem Polariodfilter, geschickt wird. Die Polarisationsachse des Strahls wird durch die Ausrichtung der Polarisationsapparatur bestimmt. Aus dem Strahl werden dann einzelne polarisierte Photonen entnommen. Durch das spezifische Verhalten von Quanten verändert das Photon seine Polarisation nach der Messung. Diese Eigenschaft ist ein großer Bestandteil des Quantenschlüsselaustauschs. Weitere Informationen über die Polarisation und das Verhalten von Photonen finden sich in [5, S. 8].
Der Quantenkanal wird in der Quantenkryptographie nicht verwendet, um Nachrichten zu senden, sondern um einen Vorrat an zufälligen Bits zwischen zwei oder mehreren Benutzern zu generieren. Im Anschluss wird durch das Vergleichen der Bits über einen gewöhnlichen Nicht-Quantenkanal überprüft, ob der Quantenkanal abgehört beziehungsweise die Kommunikation gestört wurde. Wurde die Übertragung nicht gestört, werden die erzeugten Bits, zum Beispiel als „One-Time-Pad“, für die nachfolgende Kommunikation zur Verschlüsselung genutzt. Ist das Ergebnis des Vergleichs, dass die Kommunikation gestört wurde, wird der Austausch der Quanten wiederholt, bis genügend Zufallsbits zur Verschlüsselung erzeugt wurden. [5]
Bei dem BB84-Protokoll, das 1984 von den Wissenschaftlern Charles H. Bennett und Gilles Brassard vorgeschlagen wurde, wählt ein Benutzer („Alice“) eine zufällige Bit- und Polarisationsfolge (geradlinig oder diagonal). Daraufhin sendet Alice dem anderen Benutzer („Bob“) eine Folge von Photonen. Je nach Polarisation des Photons wird dieses als binäre Null oder binäre Eins interpretiert. Dabei steht beispielsweise ein horizontal oder ein 45° ausgerichtetes Photon für eine binäre Null und ein vertikal oder 135° ausgerichtetes Photon für eine binäre Eins. Für jedes Photon, das Bob empfängt, entscheidet er unabhängig von Alice, welche Polarisation, geradlinig oder diagonal, Bob messen möchte. Daraufhin interpretiert er das Ergebnis der Messung als binäre Null oder binäre Eins. Wird versucht, die diagonale Polarisation eines geradlinigen Photons oder andersherum, zu messen, gehen alle Informationen verloren. Somit erhält Bob vorraussichtlich nur von der Hälfte der gesendeten Photonen, bei denen er die richtige Polarisationsbasis erraten hat, aussagekräftige Daten. Des Weiteren besteht die Möglichkeit, dass bei der Übertragung Photonen verloren gehen oder nicht von Bobs Detektoren erkannt werden können. [5]
Die folgenden Schritte des Protokolls finden über einen gewöhnlichen öffentlichen, nicht abhörsicheren, aber für das Verändern oder das Einspeisen von Nachrichten unanfälligen Kommunikationskanal statt. Anfangs tauschen sich Alice und Bob über die erfolgreich empfangenen Photonen aus. Dabei werden diese hervorgehoben, bei denen Bob die korrekte Polarisationsbasis erraten hat, weil nur diese zur Erzeugung des geheimen Schlüssels genutzt werden. War die Quantenübertragung ungestört, sind sich Alice und

Bob über die von den Photonen kodierten Daten einig. Niemand außer Alice und Bob hat somit die Information, ob ein beispielsweise geradlinig polarisiertes Photon horizontal oder vertikal war. Jedes Abhören birgt das Risiko, dass es bei einigen Bits zu Unstimmigkeiten zwischen Alice und Bob kommt, obwohl sie von einer Übereinstimmung ausgehen. Dies liegt an der zufälligen Mischung aus geradlinig und diagonal polarisierten Photonen. Genauer gesagt, wenn der Abhörer („Eve“) einen Lauschangriff ausführt, fängt sie jedes, von Alice gesendete Photon ab, und misst es wie Bob in einer der zwei möglichen Polarisationsbasen. Daraufhin schickt Eve das gemessene Ergebnis weiter an Bob. Bei Eves Messung gibt es zwei mögliche Fälle. Entweder misst Eve in der gleichen Basis, in der Alice das Photon gesendet hat, oder Eve misst in der anderen Basis. In dem Fall, dass Eve die richtige Polarisationsbasis gewählt hat, merken Alice und Bob nichts und Eve kennt das Bit. Misst Eve jedoch in der falschen Basis, stört Eve die Messung von Bob, wodurch Bob mit einer Wahrscheinlichkeit von 50% ein falsches Bit empfängt. [5]
Aufgrund der Tatsache, dass Eve weder die gewählten Polarisationsbasen von Alice noch die von Bob kennt, kommen beide Fälle mit gleicher Häufigkeit vor. Aus diesem Grund sind im Mittel 25% aller Bits fehlerhaft. Um zu überprüfen, ob ein Lauschangriff stattgefunden hat, wählen Alice und Bob einige der Bits aus und vergleichen cica 1/3 der korrekt empfangenen Bits über den unsicheren Kanal. Mit Hilfe von statistischen Tests kann so eine Abschätzung der Fehlerrate gewonnen werden. Ist diese zu hoch, muss davon ausgegangen werden, dass ein Lauschangriff stattgefunden hat. Daraufhin sollte die Schlüsselübertragung erneut durchgeführt werden. [5]

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Abbildung 2.1: Beispiel für den Quantenschlüsselaustausch nach dem BB84-Protokoll [5, S.9]

In Abbildung 2.1 ist ein Beispiel für einen Quantenschlüsselaustausch nach dem BB84-Protokoll zu sehen. In der ersten Zeile der Abbildung sind die zufälligen Bits von Alice und in der zweiten Zeile die dazu zufällig gewählten Polarisationsbasen dargestellt. Die dritte Zeile zeigt die Polarisation der gesendeten Photonen. Zeile vier und fünf bilden die gewählten Empfangsbasen und die daraus resultierenden empfangenen Bits ab.

Danach werden über den öffentlichen Kanal die Polarisationsbasen der empfangenen Bits ausgetauscht. Die richtigen Basen werden daraufhin von Alice bestätigt. Wenn kein Lauschangriff stattgefunden hat, sind in Zeile acht die ausgetauschten Bits dargestellt. Um zu überprüfen, dass kein Lauschangriff stattgefunden hat, tauscht Bob einen Teil der empfangenen Bits mit Alice aus. Alice überprüft diese dann auf Richtigkeit. Die restlichen, nicht über den Kommunikationskanal veröffentlichten, ergeben den Schlüssel zur Verschlüsselung der Daten.

2.2.2 Coherent One- Way- Protokoll

Ein praktisches System zu entwickeln, das zuverlässig und gleichzeitig schnell, aber auch nachweislich sicher ist, ist eine weitere Herausforderung, vor der die Forschung über den Quantenschlüsselaustausch steht. Das Coherent One-Way-Protokoll ist eine Verbesserung in diese Richtung. Ziel ist es, die Schnelligkeit des Quantenschlüsselaustausches zu verbessern, indem die Ankunftszeit eines Pulses ohne verlustbehaftete optische Elemente bei dem Empfänger („Bob“) gemessen wird. Dabei wird die Sicherheit durch die Überprüfung der Quantenkohärenz erreicht, da die Abnahme der Kohärenz auf die Anwesenheit eines Lauschers („Eve“) zurückzuführen ist. Es werden dabei von einem Lauscher Informationen über einzelne Bitwerte für den Preis der Einführung von Fehlern erlangt. [9]

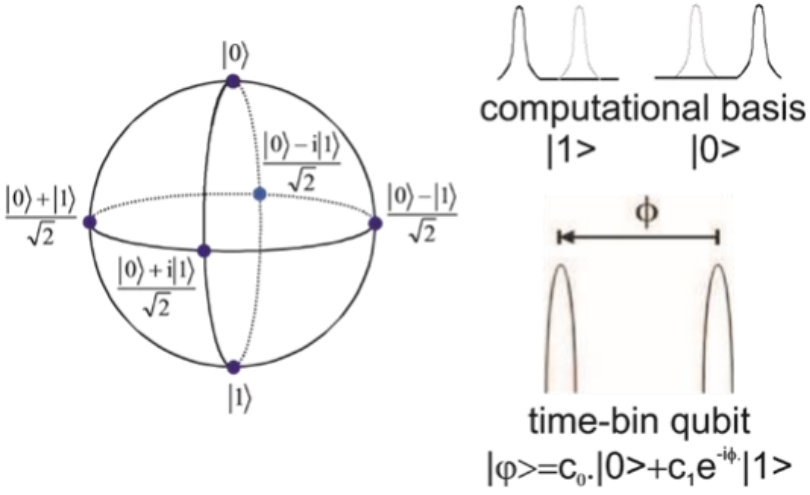

Abbildung 2.2: Illustration der Qubit-Sphäre und der Time-Bin-Qubits [10, S.29]

Es gibt verschiedene Möglichkeiten, Bits mit Hilfe von Photonen zu kodieren. Eine dieser Möglichkeiten nennt man Time-Bin-Qubits. In der Abbildung 2.2 ist zu sehen, dass diese Methode darin besteht, ein Paar kohärenter Pulse zu erzeugen. Diese breiten sich in demselben räumlichen Modus, durch eine bestimmte Zeit getrennt, aus. Dabei werden zwei Pulse genutzt. Der erste wird als früher Puls und der zweite als später Puls bezeichnet. Das Intensitätsverhältnis dieser beiden Pulse kann zwischen null und un-

endlich variiert werden, damit alle möglichen Zustände der Qubit-Sphäre erzeugt werden können. Die Extremfälle bilden somit die beiden Pole der Qubit-Sphäre. Entweder ist die gesamte optische Energie in dem frühen oder in dem späten Puls enthalten. Die Berechnungsbasis des Qubit-Raums wird durch diese beiden Quantenzustände gebildet. Wird das Verhältnis des Energieniveaus zwischen den beiden optischen Pulsen geändert, wird der Qubit-Zustand entlang der Meridiane der Qubit-Sphäre bewegt. Die Bewegung entlang der Parallelen wird durch Änderung der Phasenbezeichung zwischen frühem und spätem Puls realisiert. Ein unsymmetrisches Mach-Zehnder-Interferometer, bei dem das Eingagsstrahlteilerverhältnis variiert werden kann und der Ausgangsstrahlrekombinator ein schneller Schalter ist, ist eine Möglichkeit auf der ein Time-Bin-Qubit-Emitter basieren kann. Eine Implementierung des Time-Bin-Qubit-Analysators kann auf einem Mach-Zehnder-Interferometer basieren, bei dem Eingangs- und Ausgangsport vertauscht sind. [10]
Mit Hilfe von Time-Bin-Qubits kann das BB84-Protokoll als Coherent One Way-Protokoll implementiert werden. Die vier Qubit-Zustände befinden sich auf der äquatorialen Ebene der Qubit-Sphäre, damit möglichst viele Ähnlichkeiten in der Implementierung zu den beiden Polarisationsbasen des BB84-Protokolls gewährleistet werden. Somit bestehen die beiden Mach-Zehnder-Interferometer aus jeweils zwei 50/50- Kopplern und einem Phasenmodulator. Diese Implementierung erfordert eine starke Kontrolle über die Stabilität der Interferometer oder eine dynamische Anpassung eines Interferometers an das andere. [10]
Ziel des Coherent One Way-Protokolls ist, die Implementierung eines Quantenschlüsselaustauschsystems zu vereinfachen, um die geheime Schlüsselrate soweit zu erhöhen, dass die Industrialisierung des Systems möglich ist. Aus diesem Grund ist eine Anforderung an das Protokoll, ein einziges Interferometer zu benutzen, um die Stabilisierung des Interferometers im Vergleich zu dem anderen zu vermeiden. Eine zweite Anforderung an das Protokoll ist es, schwache kohärente Pulse zu verwenden, aber nicht Einzelphotonpulse. Dies liegt an der, im Gegensatz zu Einzelphotonquellen, simplen Implementierung von schwachen kohärenten Pulsquellen durch attenuierte Laser. [10]
Eine Besonderheit des Coherent One-Way-Protokolls ist das Verwenden der Qubit-Basen aus dem frühen und dem späten Puls. Die Messmethode zur Analyse dieser Basis ist die Messung des Zeitpunktes der Detektion des optischen Pulses. Findet eine Detektion in dem frühen Time-Bin statt, ist das Qubit ein $|0\rangle$- Zustand. Findet die Detektion hingegen in dem späten Time-Bin statt, ist das Qubit ein $|1\rangle$- Zustand. Für diese Messmethode werden keine komplexen optischen Komponenten benötigt. Das Einzige, was benötigt wird, ist ein Einzelphotonendetektor mit einer zeitlichen Genauigkeit, um zwischen den beiden Time-Bins zu unterscheiden. [10]
Auch in diesem Protokoll werden zwei Qubit-Basen verwendet, um die Sicherheit der übertragenen Schlüssel zu gewährleisten. Dabei wird die eine Basis verwendet, um den Rohschlüssel zu erzeugen und die andere, um das Sicherheitsniveau der ausgetauschten Qubits zu schätzen. Aufgrund der Verwendung eines einzelnen Detektors ist die Basis, die für den Austausch des Rohschlüssels verwendet wird, die rechnerische Basis. Diese Basis wird meistens zur Maximierung der Rohschlüsselrate genutzt. Die zweite genutzte Basis befindet sich auf der äquatorialen Ebene der Qubit-Sphäre. Der Analysator für

diese Basis ist mit einem unbalancierten Interferometer implementiert. Das Coherent One-Way-Protokoll basiert auf einem Qubit-Emitter, der kein Interferometer benötigt. Dieser Emitter muss fähig sein, entweder frühe oder späte Pulse zu emittieren. Dies kann durch Ein- und Ausschalten einer Lichtquelle in Abhängigkeit zu dem gewünschten Qubit-Zustand geschehen. [10]
Eine Schlüsselidee ist es, die Kohärenz zwischen zwei aufeinanderfolgenden optischen Pulsen, die zu demselben oder nicht zu demselben Time-Bin-Qubit gehören, zu behalten. Ist der zeitliche Abstand zwischen zwei Time-Bin-Qubits gleich der Zeit zwischen den Pulsen eines Qubits, kann die Kohärenz mit dem Interferometer in der Empfangsstation überprüft werden. Aus diesem Grund muss der Sender die gleiche Phasenbeziehung zwischen aufeinanderfolgenden optischen Pulsen, egal ob sie zu dem selben Qubit gehören oder nicht, garantieren. Zur Erhöhung der Sicherheit des Coherent One-Way-Protokolls, wird regelmäßig ein Qubit-Zustand der zweiten Basis des Empfängers emittiert. Dieser Zustand wird als Decoy-Sequenz bezeichnet. Sie besteht aus einem frühen und einem späten optischen Puls mit dem gleichen Energieniveau. Die Phasenbeziehung zwischen einem der beiden Pulse der Decoy-Sequenz und den folgenden Pulsen muss identisch zu der zwischen den Pulsen der Berechnungsbasis sein. Die Decoy-Sequenz wird mit der zweiten Basis im Empfänger analysiert, um die Sicherheit des Rohschlüssels abzuschätzen. [10]
Zusammenfassend ist das Coherent One-Way-Protokoll in Abbildung 2.3 dargestellt. Es besteht daraus, dass ein Emitter Qubit-Zustände oder Decoy-Sequenzen emittiert. Die Phasenbeziehung und die Zeit zwischen aufeinanderfolgenden Pulsen wird konstant gehalten. Das Verhältnis der Anzahl zwischen Qubits aus der Berechnungsbasis und der Anzahl an Decoy-Sequenzen fällt zugunsten der Berechnungsbasis aus. Die Empfangsstation besteht aus einem Analysator für die Berechnungsbasis und einem zur Überprüfung der Phasenbeziehung von zwei aufeinanderfolgenden optischen Pulsen. Indem die Wahrscheinlichkeit für einen Fehler im Austausch von Qubits gezählt wird, wird ein Qber-Wert (Quantum Bit Error Rate) gemessen. Die Phasenbeziehung wird, mit Hilfe des Messens der Sichtbarkeit von Interferenzen in dem zweiten Basis-Analysator, überprüft. Dieser Wert wird auch als „Visibility“ bezeichnet. Basierend auf diesen Werten wird abgeschätzt, ob die Extraktion von geheimen Schlüsseln, aus den zwischen Sender und Empfänger ausgetauschten Qubits, möglich ist. [10]
Weitere Informationen über das Coherent One-Way-Protokoll finden sich in Quelle [9].

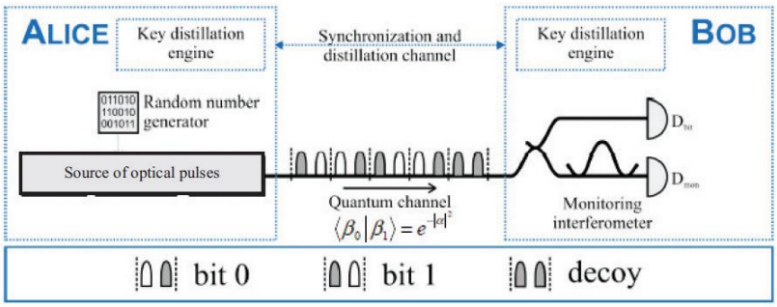

Abbildung 2.3: Illustration des Coherent One-Way-Prinzips [10, S.31]

Kapitel 3

Projekt MuQuaNet, Clavis^3 und Versuchsaufbau

Dieses Kapitel dient dazu, einen kurzen Einblick in das Projekt MuQuaNet zu geben. Weiterhin werden hier die Quantenschlüsselverteilungsplattform und die mitgelieferte Steuersoftware vorgestellt sowie die in der Software abgebildeten Werte erklärt. Außerdem werden der Versuchsaufbau und die Methodik beschrieben sowie die Darstellung der gewonnenen Daten durch die Versuchsreihen charakterisiert.

3.1 Projekt MuQuaNet

Bei dem Projekt MuQuaNet handelt es sich um ein Projekt, welches sich als Ziel gesetzt hat, ein Quantenkommunikationsnetzwerk zwischen der Universität der Bundeswehr München, dem Forschungsinstitut Cyber Defence (CODE), der zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), der Ludwig-Maximilian-Universität München sowie dem Deutschen Luft- und Raumfahrtzentrum (DLR) aufzubauen. Die Leitung des Projektes übernimmt die Universität der Bundeswehr München, genauer Prof. Dr. Udo Helmbrecht. Das Kommunikationsnetz soll nach und nach auch weiteren Einrichtungen, Behörden und militärischen Stellen zugänglich gemacht werden. Die Zeitspanne des Projekts beläuft sich vom 01.10.2020 bis zum 31.12.2024. [4]
Im Zentrum des Projektes stehen zwei verschiedene Anwendungsfälle. Zum einen die zivile Anwendung mit ADRIAN (Authority-Dependent Risk Identification and Analysis in online Networks) und zum anderen ein militärisch motivierter Anwendungsfall. [4]
Das Ziel der Anwendung ADRIAN ist es, ausgewählte Apps zu überwachen und die gesammelten Daten zu analysieren. Dies dient dazu, potenzielle Ziele zu identifizieren und deren Gefährdungspotenzial einzuschätzten. Dabei werden äußerst sensible Daten generiert und mit bereits für Sicherheitsbehörden und militärische Dienstellen gewonnenen Daten korreliert. Daraus lässt sich eine Gefährdungsplausibilität für entsprechende Personen und Standorte abschätzen. Bei den gewonnenen und verwendeten Daten bedarf es, aufgrund des Risikos, einer hochsicheren Verschlüsselung. Diese Verschlüsselung soll mit dem Quantenschlüsselaustausch realisiert werden. [4]

Bei der militärischen Anwendung soll die Fernwartung verschiedener Systeme durch den Quantenschlüsselaustausch abgesichert werden. In dem Projekt soll ein Roboter, über eine durch den Quantenschlüsselaustausch abgesicherte Verbindung, ferngesteuert und gegebenenfalls dessen Firmware aktualsiert werden. Dies gilt als „Proof of Concept“, um diese Methodik in der Zukunft auf sich im Einsatz befindende Systeme anzuwenden. Als Beispiel ist hier das Aktualisieren der Firmware von eingebetteten, militärischen Systemen mittels sicherer Fernwartung über das Quantenschlüsselaustausch-Netz zu nennen. Weiterhin beinhaltet das Projekt den Aufbau einer Freistrahlstrecke und die Anbindung von Satellitenkommunikation über das DLR. [4]
In der Abbildung 3.1 ist das Kommunikationsnetz zu erkennen. Dabei ist das Projekt MuQuaNet durch die gelbe Linie dargestellt, wobei die gelben Vierecke die verschiedenen Einrichtungen, zwischen denen das Netz aufgebaut werden soll, darstellt. Die gestrichelten Linien sollen im Rahmen einer bayerischen Studie, der „QuKOMM“ realisiert werden.

Abbildung 3.1: Projekt MuQuaNet [6]

3.2 Vorstellung der Quantenschlüsselverteilungsplattform

Die Quantenschlüsselverteilungsplattform Clavis^3 wurde als ein vielseitiges Forschungswerkzeug für akademische und technologische Laboratorien von ID Quantique entwickelt und hergestellt.
Die Quantenschlüsselverteilungsplattform besteht aus zwei Geräten. Zum einen aus der Sendeeinheit Clavis3-A und zum anderen aus der Empfängereinheit Clavis3-B. Beide Stationen besitzen eine optische und eine elektronische Steckverbindung, welche über einen Ethernet-Anschluss mit einem externen Computer verbunden sind. [7]
Die Einheiten sind über einen Quantenkanal und über einen Servicekanal verbunden. Auch sind die beiden Kanäle mit SFP-Transceivern (engl. „small form-factor pluggable“) ausgestattet und werden über Glasfaserstränge mit unterschiedlichen Steckverbindungen miteinander verbunden. Der Quantenkanal wird für die Schlüsselübertragung

verwendet und hat eine APC-Steckverbindung (englisch „angled physical contact“), wobei der Servicekanal für die Synchronisation zwischen den beiden Einheiten verwendet wird und eine LC-Steckverbindung (englisch „lucent connector“) besitzt. Beide Kanäle können auf einen einzigen SFP-Transceiver, der bidirektionale Übertragungen unterstützt, reduziert werden. Der sichere Quantenschlüsselaustausch ist über Glasfaserkabel mit einem optischem Verlust von bis zu 12 dB möglich. Dies entspricht bis zu sechzig Kilometern. Der physikalische Aufbau der Geräte findet sich in Quelle [10, S. 32]. [7]
Clavis^3 besitzt auch ein integriertes Schlüsselmanagementsystem, das Schlüsselanfragen und den Schlüsseltransfer zwischen der Quantenschlüsselverteilungsplattform und externen Verschlüsselungsgeräten verwaltet. Die Schlüsselverteilung erfolgt über eine gesicherte QKD ETSI REST API (englisch „quantum key distribution european telecommunications standards institute representational state transfer application programming interface“) oder eine selbstentwickelte proprietäre Schnittstelle. Auch kann an die Einheit Clavis3-B ein externer Einzelphotonen-Detektor angeschlossen werden. Eine Software automatisiert den Hardware-Betrieb und die komplette Schlüsseldestillation. [7]
Die Quantenschlüsselverteilungsplattform basiert auf dem „Coherent One Way (COW)-Protokoll“, welches in Kapitel 2.2.2 erklärt wird. [7]
Nach dem Austausch des Schlüssel-Rohmaterials findet das „Post- Processing“, also die Nachbearbeitung des Schlüssel-Rohmaterials, statt. Die Nachbearbeitung dient der Fehlerkorrektur und der Minimierung der Informationen, auf die ein Angreifer Zugriff haben könnte. Das „Post-Processing“ ist bei der Quantenschlüsselverteilungsplattform Clavis^3 vollständig implementiert, um einen sicheren Schlüsselaustausch zu gewährleisten. Es besteht aus fünf verschiedenen Schritten : dem „Sifting“, dem Schlüsselabgleich, der Datenschutz-Verstärkung, der Authentifizierung und der Schlüsselmaterialspeicherung und -verwaltung. [7]
Bei dem „Sifting“ werden die Bits entfernt, die nicht für den Schlüssel verwendet werden können, wie zum Beispiel die Bits aus Täuschungssequenzen und Bits, bei denen die Basen von Sender und Empfänger nicht übereinstimmen. Bei dem Schlüsselabgleich wird der „Low Density Parity Code-Algorithmus“ verwendet um Fehler zu entfernen. Dieser Algorithmus wird auch zur Schätzung der Bitfehlerrate verwendet. Bei der Datenschutz-Verstärkung wird das „Wegman-Carter Strongly Universal Hashing“ verwendet, um die möglicherweise zu einem Lauscher durchgesickerten Informationen auf ein Minimum zu reduzieren. Die Authentifizierung zwischen Clavis3-A und Clavis3-B wird durch ein informationstheoretisch sicheres polynomielles „Universal-Hashing“ realisiert und durch ein „One Time Pad“ verschlüsselt. Durch die Schlüsselmaterialspeicherung und -verwaltung kann jederzeit zur Verifikation, Schlüsselnutzung und weiteren Analysen auf die endgültigen Schlüssel zugegriffen werden. [7]

3.2.1 Vorstellung des QKD-Cockpits

Das QKD-Cockpit ist die mitgelieferte Steuersoftware von Id Quantique. Das Programm, welches auf dem externen Computer installiert sein muss, ermöglicht die Interaktion mit den Stationen Clavis3-A und Clavis3-B in einer graphischen Umgebung. Neben vielen

anderen Funktionen ermöglicht es den Start und das Verbinden der Quantenschlüsselverteilungsplattform, die Visualisierung der „Qber“, der „Visibility“ und der „Secret Key Rate“ sowie das Neustarten und das Ausschalten der Stationen. Die GUI der Software ist in der Abbildung 3.2 zu sehen. Zudem ist dort die Darstellung der gemessenen Daten zu betrachten. [8]

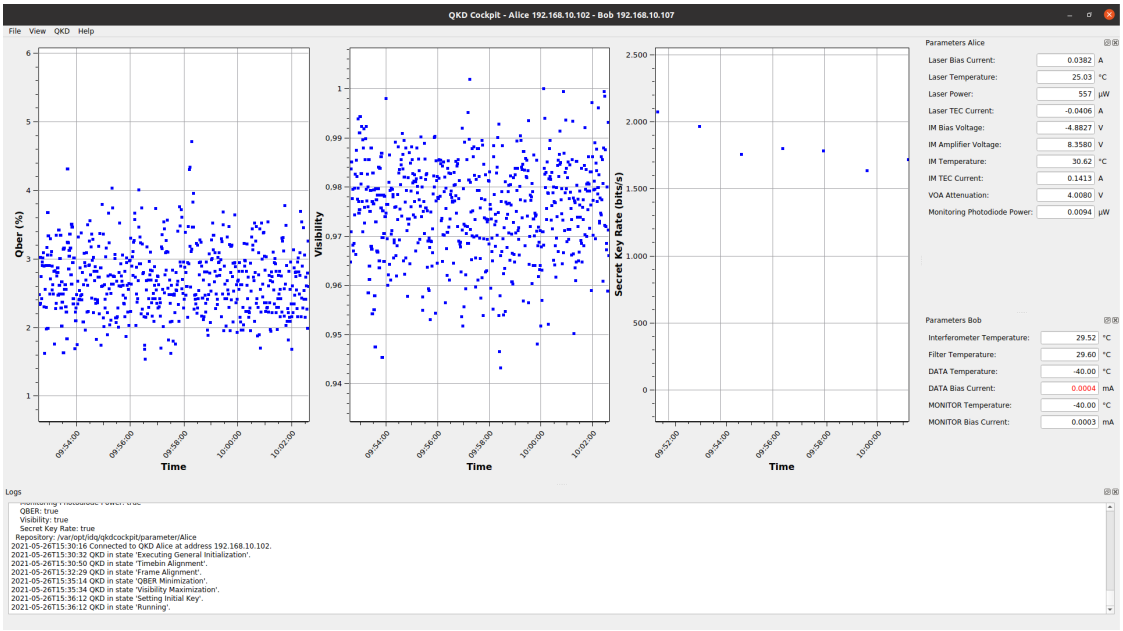

Abbildung 3.2: QKD-Cockpit

Bei jedem Neustart des Systems werden fünf Phasen durchlaufen, in denen die Stationen optimiert werden. Diese Phasen sind das „Pre-alignment“, das „Time-bin alignment“, das „Frame alignment“, die „QBER minimization“ und die „Visibility maximization“. [8]
Ziel des „Pre-alignments“ ist die Optimierung des Auslöschens zwischen leeren und nicht leeren Pulsen um dadurch eine Reduktion der „Qber“ während des Schlüsselaustausches zu erzeugen. Durch das Scannen der Modulatorvorspannung und das Auffinden der maximalen Leistung der Intensitätsmodulator-Photodiode wird die Reduktion der „Qber“ erreicht. [8]
Während des „Time-bin alignments“ wird das Erfassen von Detektierungen optimiert, indem der Erkennungspuls auf die steigende Flanke des Taktes ausgerichtet wird. Dazu wird ein festes Muster von zwanzig Bins von der Station Clavis3-A gesendet und mit Hilfe eines Flip-Flop´s resynchronisiert. Die Erkennungen werden, bis zum Erreichen des Alignment-Erkennungs-Minimums, akkumuliert und daraus wird das Verhältnis aus leeren und nicht leeren Pulsen berechnet. Die Verzögerung zwischen Takt und Detektorausgang werden mit 55 ps Schritten in der Spanne von 0 ps bis 600 ps abgetastet. Dazu werden die vorherigen Schritte immer wiederholt. Je höher das Verhältnis aus nicht leeren zu leeren Pulsen, desto besser ist die Verzögerung. [8]
Das „Frame alignment“ verfolgt das Ziel, den Offset zwischen dem Quantenkanal und

dem Servicekanal zu messen. Dieser Schritt ermöglicht es, mögliche Längenunterschiede der beiden Kanäle im Glasfaserkabel auszugleichen. Hierbei wird kontinuierlich ein festes Muster von 20 Bins von der Station Clavis3-A gesendet, wobei sich jedes 60. Muster von den anderen unterscheidet. Die Detektierungen werden erneut akkumuliert. Eine Verschiebung von 20 Bins wird zwischen dem Quanten-und dem Servicekanal eingefügt. Danach werden die vorherigen Schritte wiederholt. Diese Verschiebung von 20 Bins wird wiederholt, bis das unterschiedliche Muster erkannt wird. Wurde das Muster nicht in den 60 Mustern gefunden, wird die Verzögerung um 30*20 Bins verschoben und alle Schritte erneut durchlaufen. Wird das Muster gefunden, so wurde der Offset zwischen dem Service- und Quantenkanal gefunden. [8]
Ziel der „QBER minimization“ ist es, die Verzögerung zwischen Detektorausgang und Takt und die Vorspannung am Modulator zu optimieren um die Qber zu minimieren. [8]
Bei der „Visibility maximization“ werden der Laserstrom und die Verzögerung zwischen Detektorausgang und Takt optimiert, um die Visibility zu maximieren. [8]
Weitere Informationen über den Einstellungsprozess und die rechts in der Abbildung 3.2 angegebenen Werte finden sich in Quelle [8] ab Seite 15.

Die drei in der Abbildung 3.2 visualisierten Werte sind die „Qber“ in Prozent, die „Visibility“ in Prozent und die „Secret Key Rate“ in Bits/s.
Dabei ist „Qber“ ein prozentualer Wert, der angibt, in welchem Verhältnis fehlerhafte Bits zu den Gesamtbits des Schlüssels stehen. Diese kann durch Dunkelzählungen, Fehlausrichtungen von Polarisatoren oder Interferometern beeinträchtigt werden. Die „Qber“ wird mit der folgender Formel berechnet. [8]

$$Qber = \frac{Anzahl\ fehlerhafter\ Bits}{Gesamtzahl\ erzeugter\ Bits}$$

Die „Visibility“ ist ein relatives Maß für die Sichtbarkeit von Interferezen im zweiten Basis-Analysator. Je höher die „Visibility“, desto besser können die Photonen und Pulse detektiert werden. Die Formel zur Berechnung der „Visibility“ lautet:

$$Visibility = \frac{N(D_{M1}) - N(D_{M2})}{N(D_{M1}) + N(D_{M2})}.$$

Dabei ist $N(D_{M_1})$ definiert als Anzahl detektierter Photonen bei Detektor 1 und $N(D_{M_2})$ als Anzahl detektierter Photonen bei Detektor 2, obwohl nur Detektor 1 Photonen detektieren sollte.
Die „Secret Key Rate“ ist die Zahl der produzierten Bits eines bei Alice und Bob vorliegenden Schlüssels, der mit einer bestimmten Sicherheitsgarantie nicht von einem Eavesdropper erraten werden konnte. Diese Sicherheitsgarantie gibt eine bestimmte (sehr niedrige) höhere Schranke für die Wahrscheinlichkeit an, mit der ein Eavesdropper unter bestimmten Annahmen doch den Schlüssel abhören kann. Sowohl die Schranke als auch die Annahmen sind vom Hersteller eines QKD-Geräts zu spezifizieren. [8]

3.3 Angaben des Herstellers

Ein Mitarbeiter des Supportes der Firma ID Quantique gab mündlich Angaben über die zu erwartenden minimalen und maximalen Werte der „Visibility“, der „Qber“ und der „Secret Key Rate“ an. [11]
Laut mündlicher Aussage des Mitarbeiters liegen die besten, stabil im zeitlichen Mittelwert, zu erreichenden Werte der „Qber“ bei circa 2 Prozent und die der „Visibility“ bei circa 98 Prozent. Ab einem Anstieg der „Qber“ auf 4,5 Prozent und einen Abfall der „Visibility“ auf circa 95 Prozent, ist es der Quantenschlüsselverteilungsplattform Clavis^3, laut Mitarbeiter des Supportes, nicht mehr möglich, geheime Schlüssel zu erzeugen. [11]
Die „Secret Key Rate“ soll im Durchschnitt bei über 1400 Bits/s liegen. Diese soll in dem angegebenen Wertebereich der „Visibility“ und der „Qber“ erreicht werden. [11]
Die beschriebenen Wertebereiche sind in der Tabelle 3.1 dargestellt.

Tabelle 3.1: Darstellung der gemittelten Mindest- und Höchstwerte der „Visibility“ und der „Qber“ in Prozent sowie der „Secret Key Rate“ in Bit/s

	Mindestwert (Mittelwert)	Höchstwert (Mittelwert)
Visibility	95	98
Qber	2	4,5
Secret Key Rate	1400	/

3.4 Methodik

Bei den verschiedenen Messreihen handelt es sich um Untersuchungen zu der Stabilität der Geräte im Zeitverlauf, dem Eavesdropping-Simulator und der optischen Dämpfung. Ziel des Versuchs ist es, die Stabilität der Geräte im Zeitverlauf zu testen sowie mögliche Störungen zu beobachten. Der Versuchsaufbau wird über den gesamten Zeitraum der Messung nicht verändert.
Bei der Versuchsreihe mit dem Eavesdropping-Simulator ist es das Ziel, das Verhalten der „Qber“, der „Visibility“ und der „Secret Key Rate“ während eines simulierten Angriffs zu untersuchen. Dazu wird der Eavesdropping- Simulator an die Stationen Clavis3-A und Clavis3-B angeschlossen. Der Versuchsaufbau wird während der Testung nicht weiter verändert. Es wird lediglich die Skala des Eavesdropping-Simulators verändert.
Im Bezug auf die verschiedenen optischen Dämpfungen steht im Mittelpunkt, bis zu welcher maximalen optischen Dämpfung Schlüssel generiert werden können, sowie bei welcher optischen Dämpfung die stabilste und beste Schlüsselgenerierung stattfindet. Hierbei wird der Versuchsaufbau bei jeder Messung verändert, da die unterschiedlichen Attenuatoren ausgetauscht werden müssen.
Anschließend gilt es, aus den Erkenntnissen der Messungen neue Vermutungen zu formulieren, die den Ausgangspunkt für weitere Messreihen bilden.

Die genutzte Quantenschlüsselverteilungsplattform Clavis[3] bietet keine dazugehörige Möglichkeit, die gemessenen Daten direkt einzeln zu extrahieren. Stattdessen besteht nur die Möglichkeit, alle „Logfiles“ der Geräte auszugeben. Deshalb wurden die, für die einzelnen Graphen benötigten Daten, aus den „Logfiles“ mit Hilfe eines selbstgeschriebenen Skriptes ausgelesen. Das Programm Gnuplot diente schließlich dazu, aus den extrahierten Daten verschiedene Graphen zu erstellen.
Die „Quantum Bit Error Rate“ und die „Visibility“, liefern circa 60 Werte pro Minute. Diese werden von der mitgelieferten Steuersoftware angezeigt. Der angezeigte Ausschnitt der Datenpunkte ist zeitlich sehr begrenzt, weshalb aus den Rohdaten keine aufschlussreichen Erkenntnisse gezogen werden können. Aus diesem Grund wird ein Datenbearbeitungsschritt durchgeführt, in dem die Mittelwerte und die Standardabweichungen, über einen für die Versuchsreihe geeigneten Zeitraum, berechnet werden. Anschließend werden die bearbeiteten Daten in den verschiedenen Diagrammen dargestellt. Dabei wird die Standardabweichung der Werte für den Zeitraum durch die y-Achsen-Fehlerbalken an den Punkten, die die Mittelwerte abbilden, dargestellt.

3.5 Versuchsaufbau

Der Versuchsaufbau für die vorgenommenen Messungen ist in der Abbildung 3.3 zu erkennen. Dieser war grundsätzlich in allen Messungen gleich, nur wurden am Quantenkanal, bevor dieser in den Eingang bei der Station Clavis3-B geht, für eine Messung die Attenuatoren ausgewechselt. Attenuatoren sind Bauteile, welche optische Dämpfungen künstlich in ein System einführt. Diese werden benötigt, da ID Quantique eine optische Mindestdämpfung für die Quantenschlüsselverteilungsplattform vorgibt, damit der eingebaute Detektor nicht überlastet ("geblendet") wird. Die einzige Änderung an dem Versuchsaufbau wurde vorgenommen, als die Messung mit dem Eavesdropping-Simulator stattfand. Der Eingang des Quantenkanals des Eavesdroppers wurde an den Ausgang des Quantenkanals der Station Clavis3-A angeschlossen und der Ausgang des Quantenkanals des Eavedroppers an den Eingang des Quantenkanals der Station Clavis3-B.
Die beiden Stationen, Clavis3-A und Clavis3-B, wurden nebeneinandner aufgebaut. Der Quantenkanal der Geräte wurde mit einem FC/APC-Kabel verbunden. Der klassische Kanal der beiden Stationen wurde mit einem LC-Kabel verbunden. Über den Ethernet Anschluss wurde die Quantenschlüsselverteilungsplattform, mit Hilfe eines zwischengeschalteten Switchs, mit einem externen Computer verbunden. Den Stationen wurde mit Hilfe des Computers und des QKD-Cockpits IP-Adressen zugewiesen. Dies ermöglichte das Nutzen der beiden Stationen.

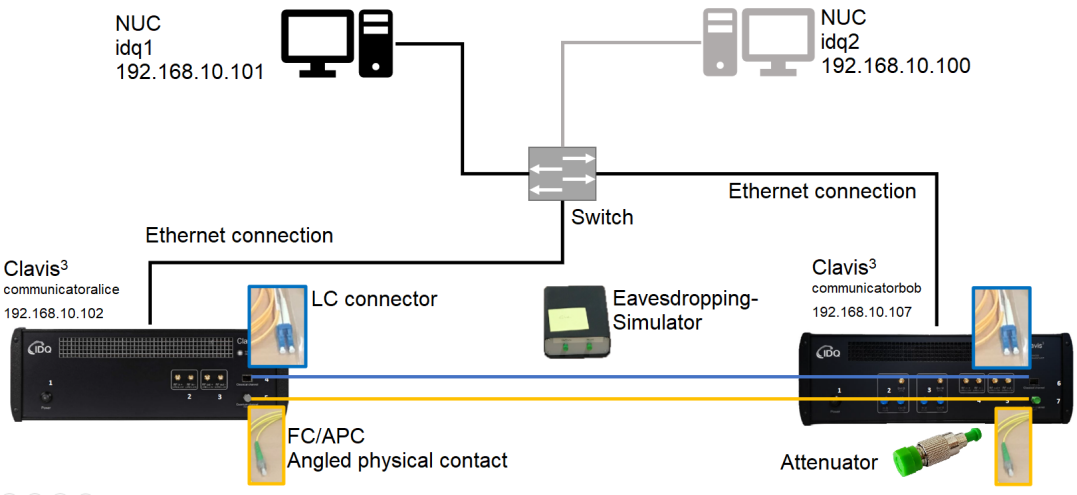

Abbildung 3.3: Versuchsaufbau [6]

Abbildung 3.4: Versuchsaufbau - Realität (nicht angeschlossen)

In der Abbildung 3.4 ist der Versuchsaufbau im Labor zu sehen. Links im Bild befindet sich die Station Clavis3-A und rechts die Station Clavis3-B. Zwischen den Stationen befindet sich der Eavesdropping-Simulator. Die gelben Kabel sind Glasfaserkabel mit APC-Steckverbindung, die an den Quantenkanal angeschlossen werden. Das orangefarbene Kabel besitzt eine LC-Steckverbindung und wird für den klassischen Kanal benutzt. Das dritte Teil von links, vor der Station Clavis3-A, ist ein Attenuator.

3.5.1 Darstellung der gemessenen Daten

Das QKD-Cockpit liefert keine Möglichkeit, die gemessenen Daten nach den Größen „Qber“, „Visibility“ und „Secret Key Rate“ sortiert zu exportieren. Aus diesem Grund wurde ein Pythonskript geschrieben, das die Logfiles ausliest und die benötigten Daten extrahiert. Dieses Skript ist im Anhang A zu finden. Der Aufbau der Logfiles ist in Abbildung 3.5 zu sehen.

```
2021-04-02T06:47:42.309 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] Visibility: 0.971954
2021-04-02T06:47:43.317 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] QBER: 0.0201847
2021-04-02T06:47:43.317 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] Visibility: 0.967002
2021-04-02T06:47:43.317 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Regulating QBER: modulator bias = -5.14695 V, QBER = 0.0232882.
2021-04-02T06:47:43.317 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Regulating visibility: laser current = 0.0399727 A, visibility = 0.974412.
2021-04-02T06:47:44.198 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Key-block filling percentage: 99.6%
2021-04-02T06:47:44.314 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] QBER: 0.0322271
2021-04-02T06:47:44.315 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] Visibility: 0.969631
2021-04-02T06:47:45.312 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] QBER: 0.0231191
2021-04-02T06:47:45.313 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] Visibility: 0.983664
2021-04-02T06:47:45.800 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Key-block filling percentage: 100.0%
2021-04-02T06:47:46.311 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] QBER: 0.0283194
2021-04-02T06:47:46.311 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] Visibility: 0.972574
2021-04-02T06:47:46.344 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Updating PA parameters: FullBlockHashValids: 512, FullBlockHashErrors:32
2021-04-02T06:47:46.345 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Updating PA parameters: rawQBER = 0.032887, dccQBER = 0.024850
2021-04-02T06:47:46.345 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Updating PA parameters: rawVIS = 0.911386, dccVIS = 0.975056
2021-04-02T06:47:46.345 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Updating PA parameters: mu = 0.031051, cr = 0.174997
2021-04-02T06:47:46.345 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Updating PA parameters: Timer = 115.020000
2021-04-02T06:47:46.345 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Updating PA parameters: Column: 4, Row: 4
2021-04-02T06:47:46.345 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Next compression ratio: 0.174997
2021-04-02T06:47:46.345 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Current compression ratio: 0.171425
2021-04-02T06:47:46.345 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Key-block rate: 1483.428955 bits/s
2021-04-02T06:47:46.345 INFO  [cervino::communicator::backend::OpticsRegulationAlice] Key-block filling percentage: 1.2%
2021-04-02T06:47:46.345 DEBUG [cervino::communicator::backend::KeyExchangeAlice] Actual key rate: 1889.95 bits/s
2021-04-02T06:47:47.309 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] QBER: 0.0269705
2021-04-02T06:47:47.309 DEBUG [cervino::communicator::backend::OpticsRegulationAlice] Visibility: 0.963914
```

Abbildung 3.5: Beispiel der auszulesenden Logfiles

Die aus den Logfiles ausgelesenen Daten wurden in eine Textdatei geschrieben, um diese mit dem Programm Gnuplot (Version 5.4 patchlevel 1 für Windows) auszuwerten.
In der Abbildung 3.6 ist die „Qber“ über einem Zeitraum von elf Minuten abgebildet. In diesem Diagramm sind 664 Datenpunkte vorhanden. Die Rohdaten weisen eine große Schwankung auf, weshalb es sinnvoll ist, auf die Mittelwertbildung zurückzugreifen. In demselben Zeitraum wurden auch 664 Datenpunkte für die „Visibility“ erzeugt, weshalb zu Demonstrationszwecken nur ein Diagramm der „Qber“ erstellt wurde.

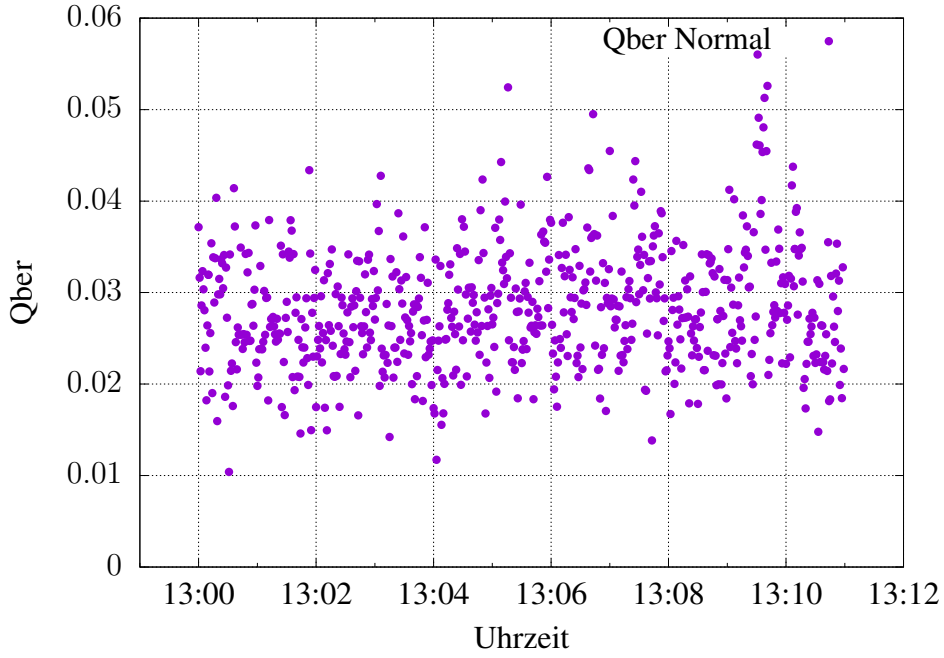

Abbildung 3.6: Darstellung der „Qber“ ohne Mittelwertberechnung

Aufgrund der Unübersichtlichkeit des Diagrammes wird zur Darstellung der Messergebnisse der folgenden Versuchsreihen der Mittelwert und die Standardabweichung über Zeiträume, die für die jeweilige Messung sinnvoll sind, berechnet. Die große Streuung der Messwerte wird in den späteren Diagrammen durch Fehlerbalken dargestellt, deren Länge durch die Standardabweichung gegeben ist. Mittelwert μ und Standardabweichung σ wurden nach den üblichen Formeln

$$\mu = \frac{1}{n}\sum_{k=1}^{n} a_k$$

und

$$\sigma = \sqrt{\frac{\sum_{k=1}^{n}(a_k - \mu)^2}{n}}.$$

berechnet, wobei $a_k,\ k = 1, ..., n$ die Datenpunkte bezeichnen. In Python sind diese über die Befehle „np.mean“ und „np.std“ der Programmbibliothek „NumPy“ implementiert.

Kapitel 4

Ergebnisse und Auswertungen der Versuche

In diesem Kapitel werden die einzelnen Versuche und ihre Rahmenbedingungen beschrieben und die entstandenen Messreihen ausgewertet. Des Weiteren wird hier auf mögliche Lösungsmöglichkeiten von aufgetretenen Problemen und Erkenntnisse zur Optimierung der Betriebsbedingungen und Schlüsselraten eingegangen.
Grundsätzlich ist die Empfindlichkeit der Glasfaserkabel und der Photondetektoren hervorzuheben, da bereits kleine Erschütterungen, Verschmutzungen oder Verkantungen die Messergebnisse negativ beeinflussen können. Zudem justiert sich die Quantenschlüsselverteilungsplattform kontinuierlich nach, sodass sich die verschiedenen Betriebsparameter, wie zum Beispiel die Spannung des Intensitätsmodulators des Lasers, Temperatur et cetera und somit die Datenpunkte im laufenden Betrieb verändern können. Auch bei jedem Neustart können die Anfangseinstellungen variieren. Die Variation der Anfangseinstellungen ist jedoch für die verschiedenen Versuchsreihen von keiner großen Relevanz, da sie nur minimale Änderungen der betrachteten Größen verursachen. Zusätzlich besitzen die gemessenen Größen „Qber“, „Visibility“ und „Secret Key Rate“ wie zum Beispiel für die „Qber“ in Abbildung 3.6 dargestellt, im normalen Betriebszustand eine große Schwankungsbreite.

4.1 Stabilitätsstudie

Ziel dieser Studie war es, herauszufinden, wie stabil die Quantenschlüsselverteilungsplattform über einen längeren Zeitraum unter verschiedenen Umständen läuft, sowie welche Besonderheiten beziehungsweise Störungen sich beobachten lassen.
Dazu wurde über den Zeitraum der einzelnen Messungen an dem Versuchsaufbau keine Änderungen vorgenommen, um das Ergebnis nicht zu beeinflussen, ledigliche äußere, nicht beeinflussbare Änderungen, wie wetterbedingte Lichteinflüsse mussten hingenommen werden. Die Rahmenbedingungen der beiden Versuchsreihen blieben dazu, bis auf äußere Faktoren, wie zum Beispiel wetterbedingte Lichteinflüsse, gleich - die Stationen waren nicht abgedeckt, der Raum wurde nicht verdunkelt und es wurde ein Attenuator mit einer optischen Dämpfung von 10 dB benutzt.

Um eine anschauliche Darstellung der gemessenen Daten zu ermöglichen, wurden der Mittelwert und die Schwankungsbreite in Zeiträumen von jeweils einer Stunde gebildet.

4.1.1 Erste Stabilitätsstudie

Bei der erster Stabilitätsstudie wurden Daten über insgesamt sechs aufeinanderfolgende Tage erhoben, ohne die Stationen manuell auszuschalten oder neuzustarten. Es wurde zu jedem Tag ein separates Diagramm der „Qber“, der „Visibility“ und der „Secret Key Rate“ erstellt. Außerdem wurden Diagramme der Größen erstellt, in denen die Ergebnisse für die verschiedenen Tage der Messung zusammen (aber der Übersichtlichkeit halber ohne Fehlerbalken) dargestellt sind. In dem folgenden Unterkapitel werden ausgewähte, besonders aussagekräftige, Diagramme gezeigt und beschrieben. Die restlichen Diagramme sind im Anhang B zu finden.
Die Diagramme der Tage zwei und fünf wurden aufgrund des sichtbaren Unterschiedes für die nähere Betrachtung ausgewählt.

In der Abbildung 4.1 ist die „Visibility“ und in Abbildung 4.2 die „Qber“ dargestellt. Das Diagramm 4.1 zeigt einen deutlichen Abfall der „Visibility“ zur Mittagszeit. Die „Qber“ steigt zur Mittagszeit jedoch an. Auch die „Secret Key Rate“ halbiert sich zwischen 09:00 Uhr und 11:00 Uhr. Wird nur dieser Tag betrachtet, ist es möglich, dass es sich hier um einen Zufall handelt. Aus diesem Grund werden auch die Diagramme des fünften Tages betrachtet.

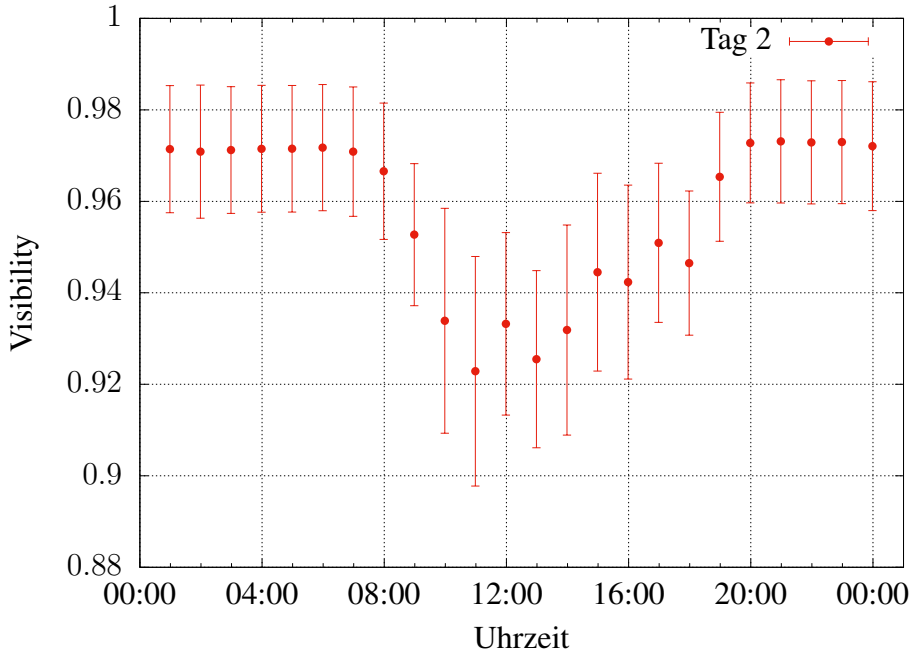

Abbildung 4.1: Tag 2 - Visibility

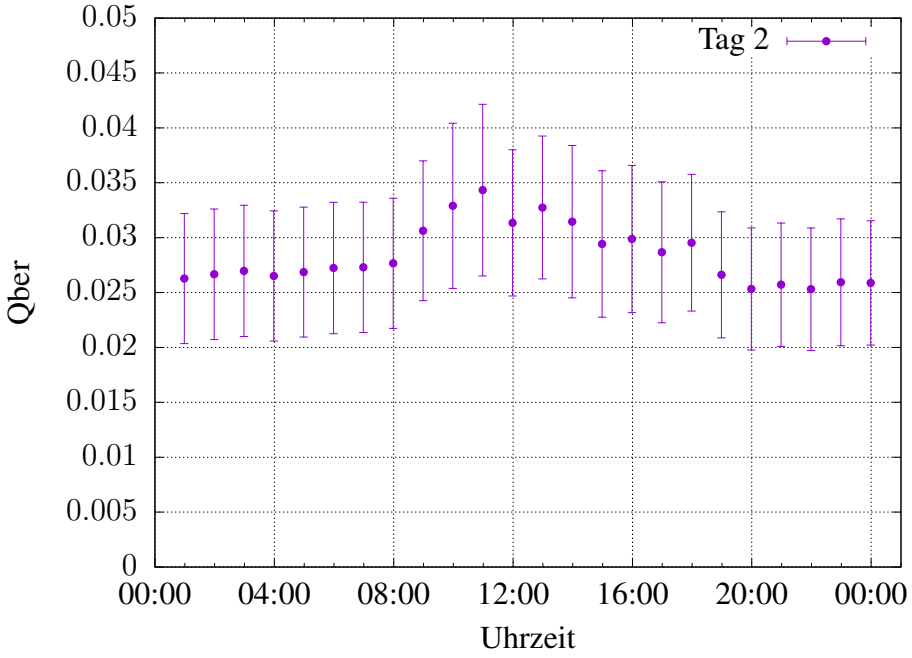

Abbildung 4.2: Tag 2 - Qber

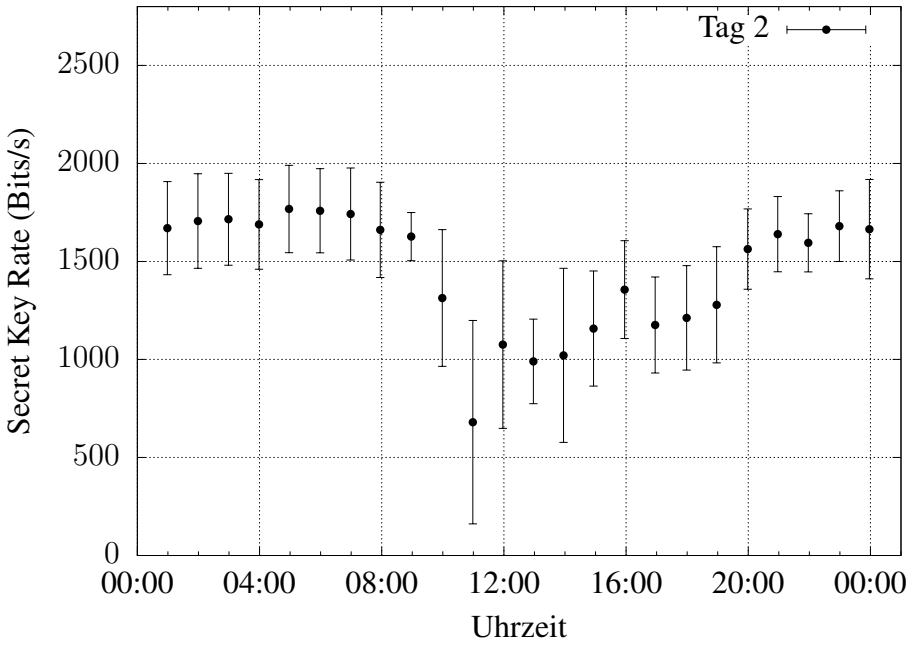

Abbildung 4.3: Tag 2 - Secret Key Rate

Bei der Auswertung der Daten des fünften Tages sind jeweils zwei Diagramme für die „Visibility“ und für die „Qber“ entstanden. Dies liegt an den großen Schwankungen der Messdaten.
In den Diagrammen 4.4 und 4.5 ist zu sehen, dass die „Visibility“ und die „Qber“ um 13:00 Uhr und 14:00 Uhr sehr niedrig beziehungsweise hoch ist. Diese Werte sprengen den Rahmen der möglichen Grenzen der Werte, sodass die Quantenschlüsselverteilungsplattform in diesen Zeiträumen keine geheimen Schlüssel produzieren konnte. Dies ist in Abbildung 4.9 zu sehen.
Aus den ausgelesenen Messdaten geht hervor, dass die „Qber“ zwischen 13:00 Uhr und 14:00 Uhr zwischenzeitlich auf ca. 50 Prozent angestiegen ist. Dadurch sieht man in dem Diagramm 4.5 um diese Uhrzeit einen unüblich hohen Wert der „Qber“ mit circa 32 Prozent und circa 19 Prozent. Dieses geht aus Abbildung 4.6 hervor.
Ebenfalls wird anhand der ausgelesenen Daten ersichtlich, dass die „Visibility“ in dem Zeitraum stark gesunken ist. Das geht auch aus Abbildung 4.4 hervor. Die „Visibility“ ist mit 69 Prozent und 80 Prozent ungewöhnlich niedrig. In diesem Zeitraum ist die „Visibility“ zeitweise auf 50 Prozent gesunken.
Zudem kann man aus den Logfiles auslesen, dass die Stationen zwischen 12:38 Uhr und 13:26 Uhr keine Datenpunkte produziert haben. In diesem Zeitraum haben sich die Geräte andauernd selbstständig neu gestartet, da die Betriebsparameter zu schlecht waren. Die Quantenschlüsselverteilungsplattform versucht sich selbständig neu einzustellen, sobald innerhalb eines bestimmten Zeitabschnitts keine oder nicht genügend Schlüsselmaterial erzeugt werden kann.

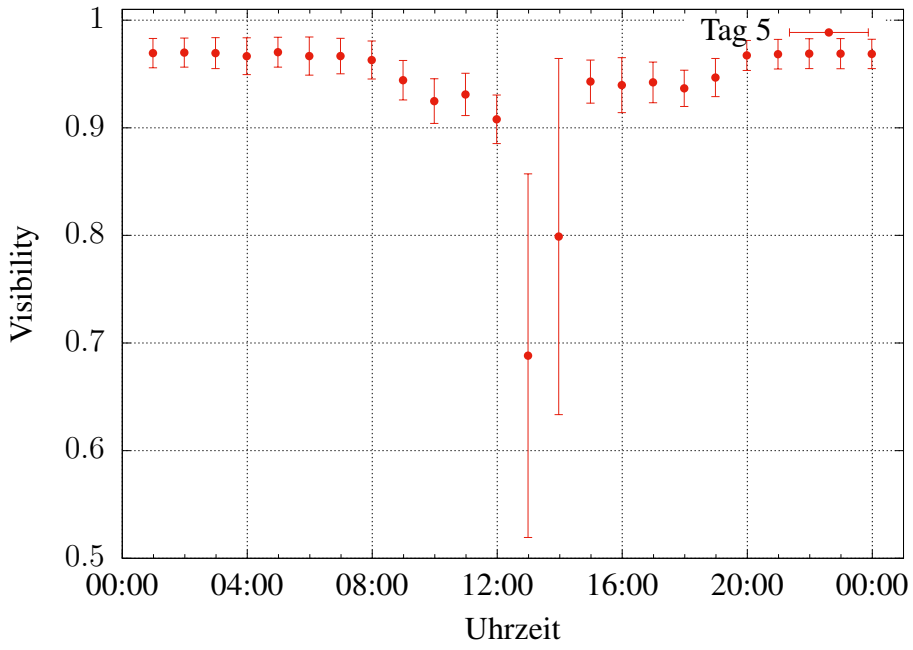

Abbildung 4.4: Tag 5 - Visibilty - Erweiterter y-Achsenbereich

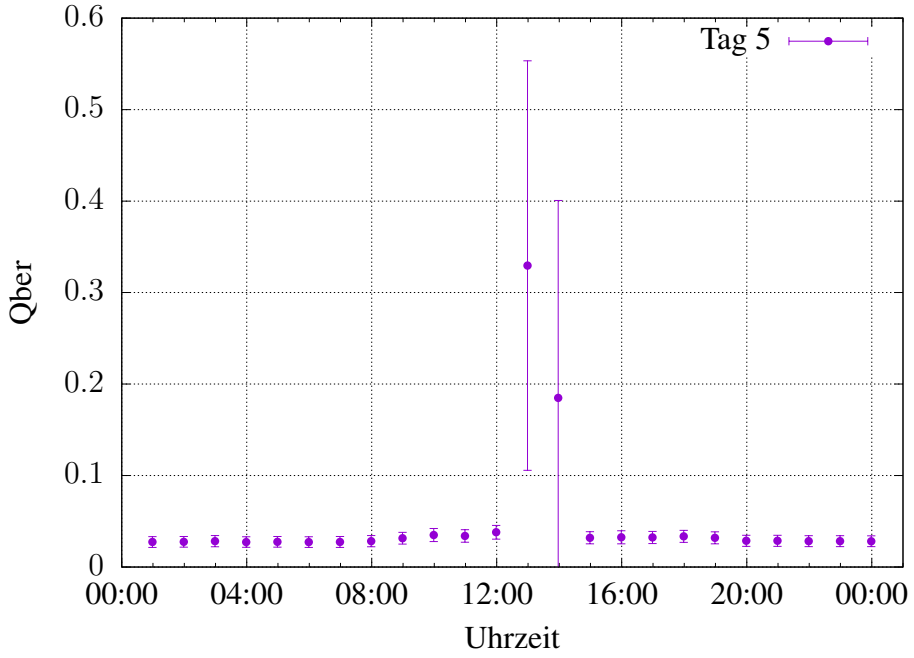

Abbildung 4.5: Tag 5 - Qber - Erweiterter y-Achsenbereich

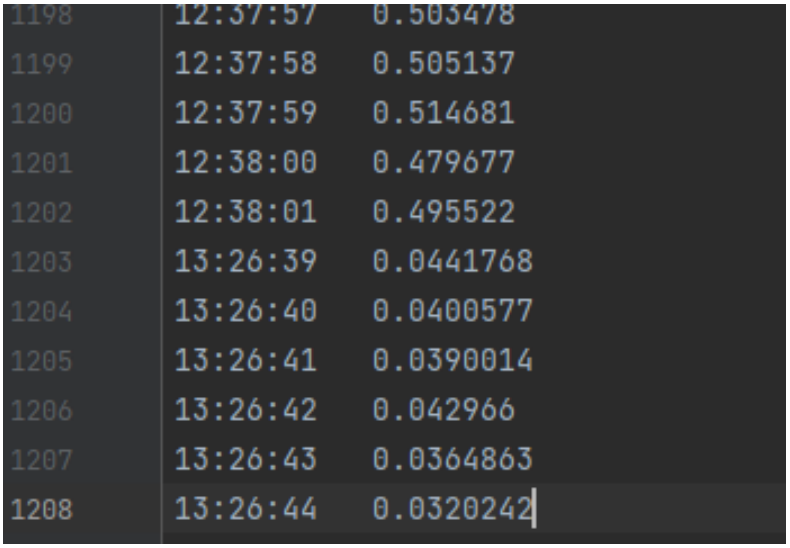

Abbildung 4.6: Qber - Hohe Datenpunkte

Aus den Diagrammen 4.4, 4.8 und 4.9 geht hervor, dass sich alle Werte zur Mittagszeit verschlechtern. Die Besonderheit im Gegensatz zum ersten Tag sind die Werte um 13:00 und 14:00. Zu diesen Zeitpunkten waren die „Qber“ und die „Visibility“ so hoch beziehungsweise niedrig, dass keine Schlüssel generiert werden konnten. Im Gegensatz zu dem zweiten Tag der Messung, schien die Sonne an den anderen Tagen deutlich intensiver. Dies verdeutlicht, dass das Tageslicht einen massiven Einfluss auf die Funktionsweise der Geräte besitzt.
Diese Erkenntnis, so einfach sie auch erscheinen mag, war für das Projektteam durchaus wichtig und überraschend, da zum Zeitpunkt der erstmaligen Installation der Clavis-Geräte Anfang Februar 2021 kein deutlicher Einfluss des Tageslichts bemerkt wurde. Das ist vermutlich auf das erheblich schwächere Tageslicht im Februar zurückzuführen. Überdies war bei punktuellen Beobachtungen über nur einige dutzende Minuten ohne Mittelwertbildung über längere Zeiträume kein so klarer Trend wie in den hier erstellten Diagrammen erkennbar.

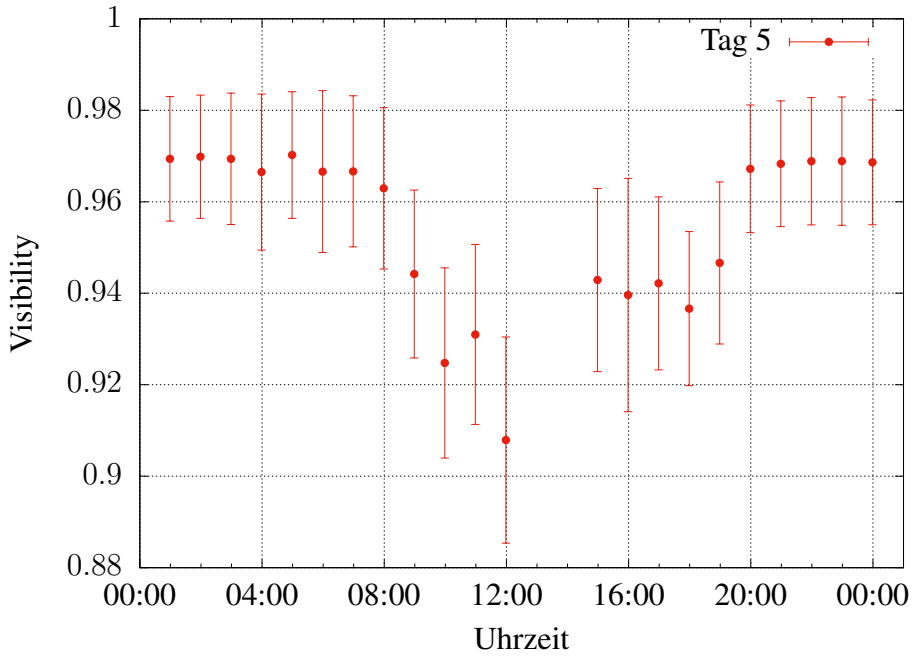

Abbildung 4.7: Tag 5 - Visibility

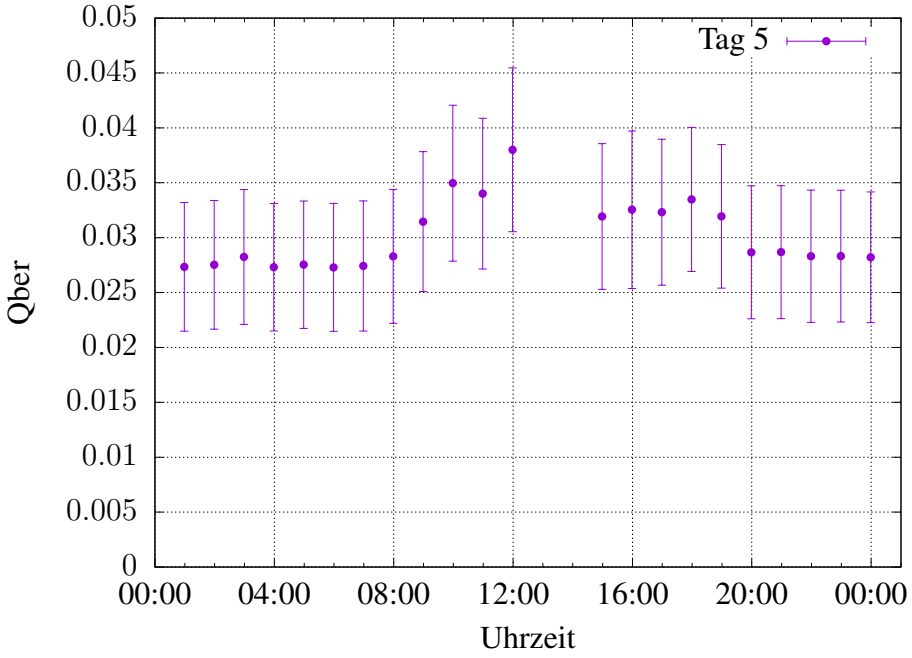

Abbildung 4.8: Tag 5 - Qber

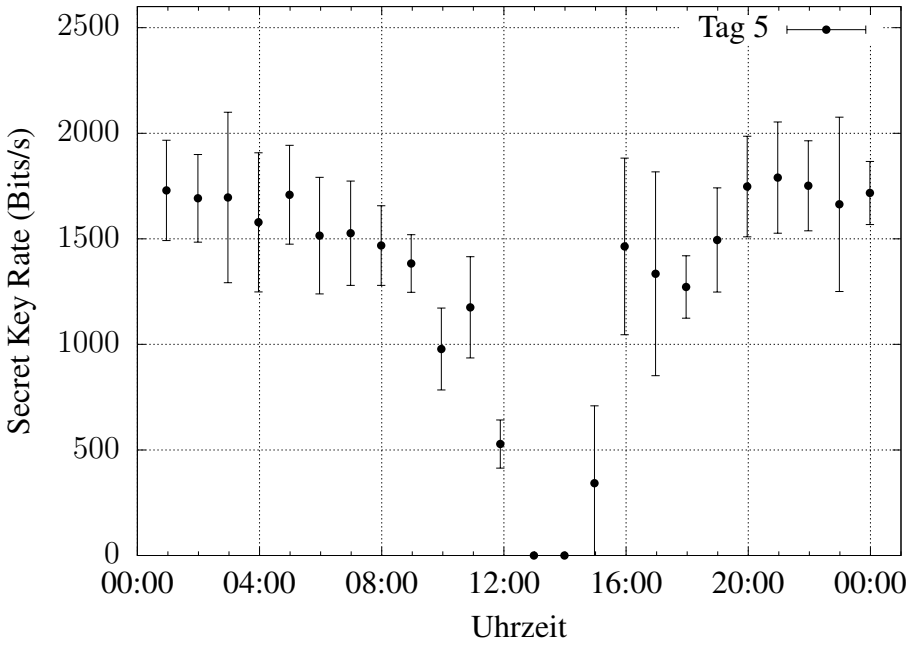

Abbildung 4.9: Tag 5 - Secret Key Rate

In den folgenden drei Diagrammen sind alle Datenpunkte von allen Tagen zusammengefasst. Man kann erkennen, dass an allen sonnigen Tagen die „Visibility“ zur Mittagszeit abfällt, die „Qber“ zur Mittagszeit ansteigt und sich die „Secret Key Rate“ in der Mittagszeit verschlechtert, beziehungsweise die Geräte nicht in der Lage waren, geheime Schlüssel zu erzeugen. Im Anhang B.0.1 findet sich eine Tabelle mit den beobachteten Wetterverhältnissen. Diese resultieren ausschließlich aus Beobachtungen und liegen keiner wisschenschaftlichen Quelle zu Grunde.
Aus diesem Diagramm lässt sich schließen, dass die Quantenverschlüsselungsplattform stark durch Tageslicht beeinflusst wird und die Detektoren durch ungewollt durchdringende Photonen des Tageslichts Fehler verursachen. Eine weitere Vermutung war, dass die Anschlüsse der Kabel oder der Attenuator defekt gewesen seien, da zum Zeitpunkt der Messungen (ohne Auswertung der Langzeitmessungen) nicht klar war, dass das Tageslicht der Hauptfaktor für Störungen war. Das Projektteam vermutete vor Auswertung dieser Messungen auch einen möglicherweise defekten Attenuator als alternative (oder zusätzliche) Störquelle. Deshalb wurde eine zweite Stabilitätsstudie durchgeführt.

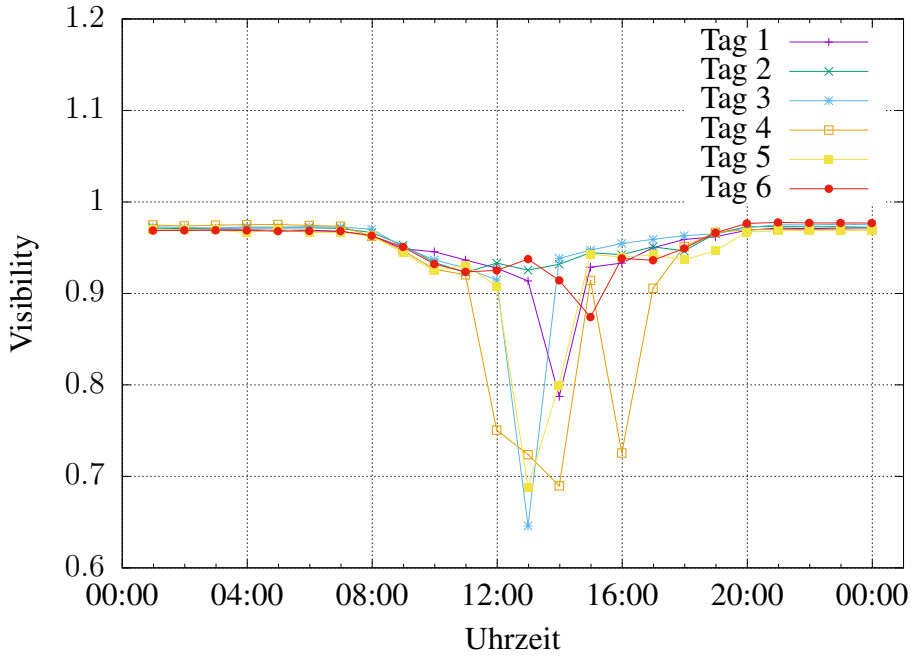

Abbildung 4.10: Tag 1-6 - Visibility

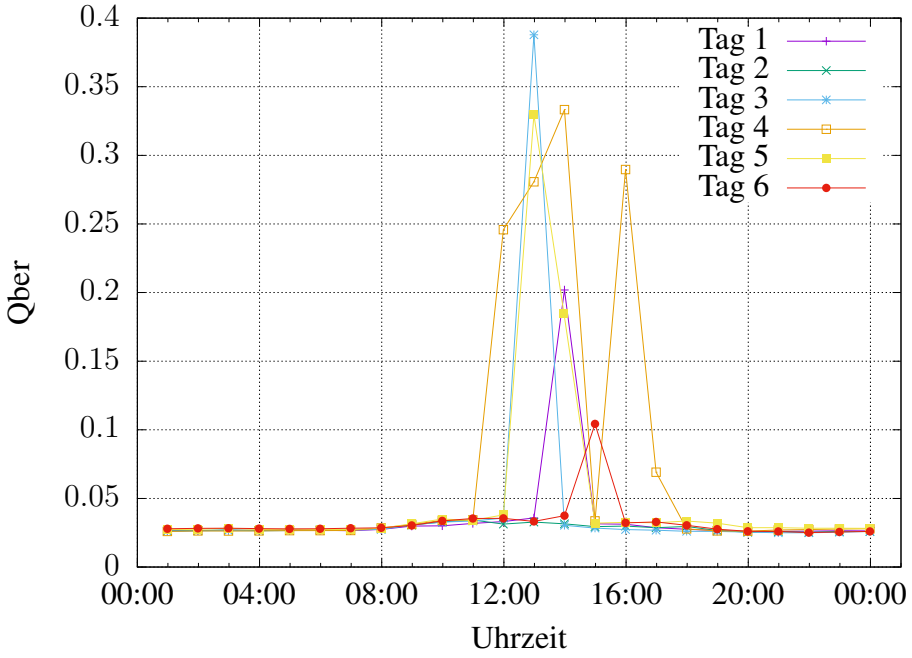

Abbildung 4.11: Tag 1-6 - Qber

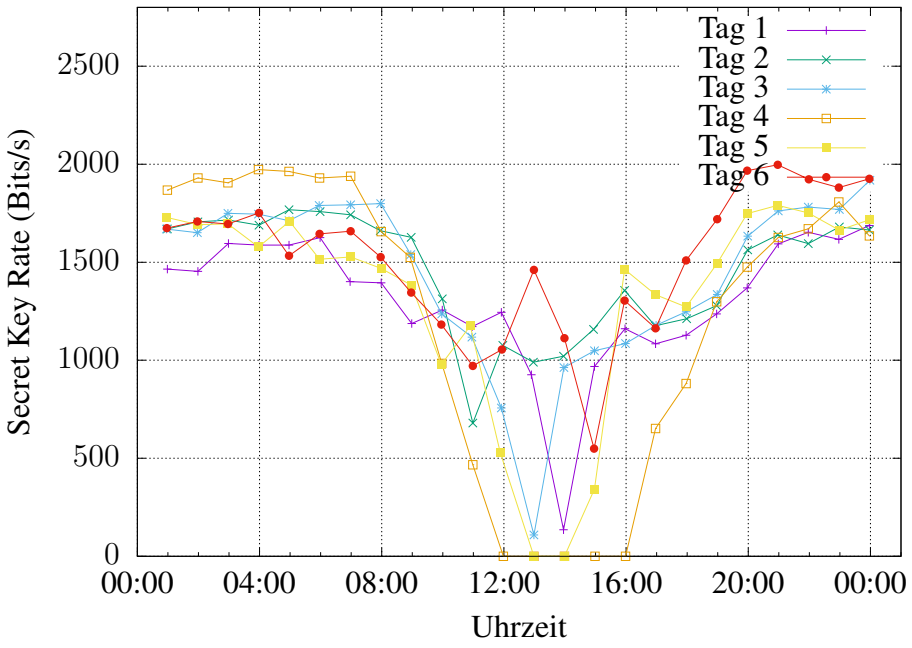

Abbildung 4.12: Tag 1-6 - Secret Key Rate

4.1.2 Zweite Stabilitätsstudie

Angesichts der Ergebnisse der ersten Messreihe galt es auszuschließen, dass die schlechten Werte der „Qber“, der „Visibility“ und der „Secret Key Rate“ durch defekte Komponenten in dem Versuchsaufbau verursacht wurden. Obendrein sollte überprüft werden, ob das Tageslicht der einzige Faktor war oder mehrere Faktoren Grund für die schlechten Werte sind. Deshalb wurden das Glasfaserkabel des Quantenkanals und der zugehörige Attenuator erneuert. Danach erfolgte die Messung mit dem neuen Glasfaserkabel und dem neuen Attenuator, der auch eine optische Dämpfung von 10 dB besitzt. Die Messdaten wurden, wie im vorigen Abschnitt beschrieben, ausgewertet. Es wurden jeweils Diagramme für die einzelnen Tage erstellt und alle Tage in einem Diagramm zusammengefasst. Die Diagramme der einzelnen Tage sind im Anhang zu betrachten.
Auch in dieser Messreihe ist zu sehen, dass sich die „Qber“ und die „Visibility“ zur Mittagszeit verschlechtern. Der Mittelwert der „Visibility“ sinkt hier maximal auf circa 57 Prozent ab. Dies ist in Abbildung 4.13 zu erkennen. Die „Qber“ steigt im Mittelwert auf maximal circa 50 Prozent an. Jenes ist in Abbildung 4.14 zu betrachten. Außerdem kann man in diesem Diagramm die parallele Veränderung von „Visibility“ und „Qber“ erkennen. Je höher die „Qber“, desto niedriger die „Visibility“. Das ist insbesondere an Tag 4 von 13:00 Uhr bis 20:00 Uhr zu sehen. Ähnliche Trends sind auch an den anderen Tagen zu erkennen.
Auch wird die Abhängigkeit der „Secret Key Rate“ von den anderen beiden Werten deutlich. Sobald die „Qber“ in ihrem Mittelwert über einen Wert von circa 4,5 Prozent ansteigt und die „Visibility“ in ihrem Mittelwert unter einen Wert von circa 90 Prozent fällt, ist es den Stationen nicht mehr möglich, geheime Schlüssel zu produzieren. Die Wertegrenze der „Qber“ stimmt mit der von dem Supportmitarbeiter angegebenen Grenze überein, die der „Visibility“ jedoch nicht. Diese ist mit circa 90 Prozent deutlich niedriger, als die von dem Supportmitarbeiter angegebene Grenze von 95 Prozent.
Nach dieser Messreihe wurde der Verdacht, dass das Tageslicht einen Einfluss auf die Stationen nimmt, erhärtet, da auch während dieser Messung die Sonne zur Mittagszeit schien und die Geräte in der Nacht stabil liefen. Im Anhang B.0.2 findet sich eine Tabelle mit den beobachteten Wetterverhältnissen. Diese resultieren ausschließlich aus Beobachtungen und liegen keiner wisschenschaftlichen Quelle zu Grunde.
Außerdem konnte durch diese Versuchsreihe ausgeschlossen werden, dass defekte Bauteile negative Einflüsse auf die Werte der „Qber“, der „Visibility“ und der „Secret Key Rate“ haben, da diese Bauteile vor der Messung erneuert wurden. Des Weiteren erhöhte sich die Stundenanzahl, an der die Sonne tagsüber schien, weswegen auch die Werte der „Qber“ und der „Visibility“ über einen längeren Zeitraum unter, die von dem Supportmitarbeiter angegebenen Mindestwerte der Größen, gefallen sind.

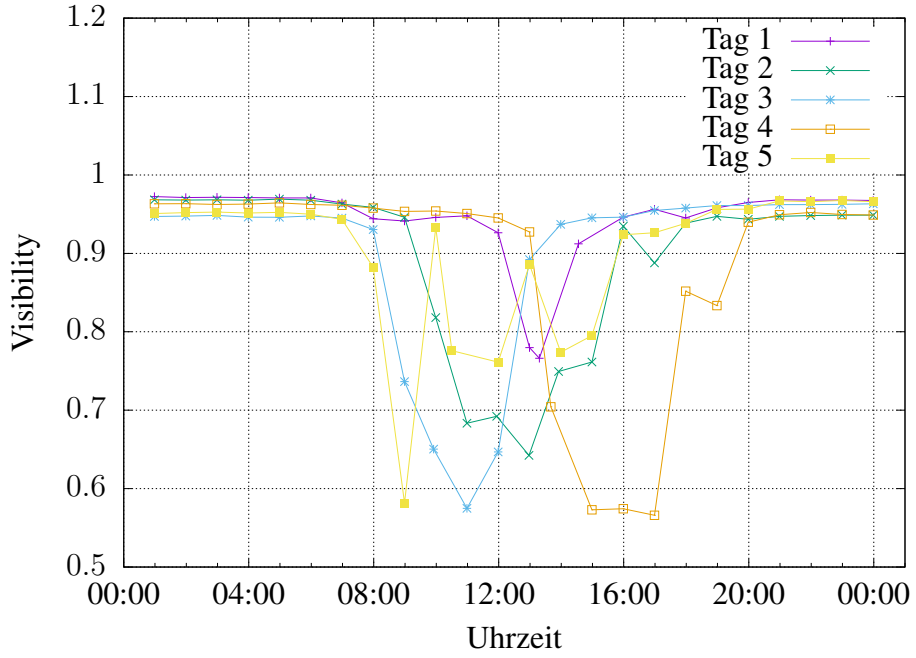

Abbildung 4.13: Tag 1-5 - Visibility - Messung 2

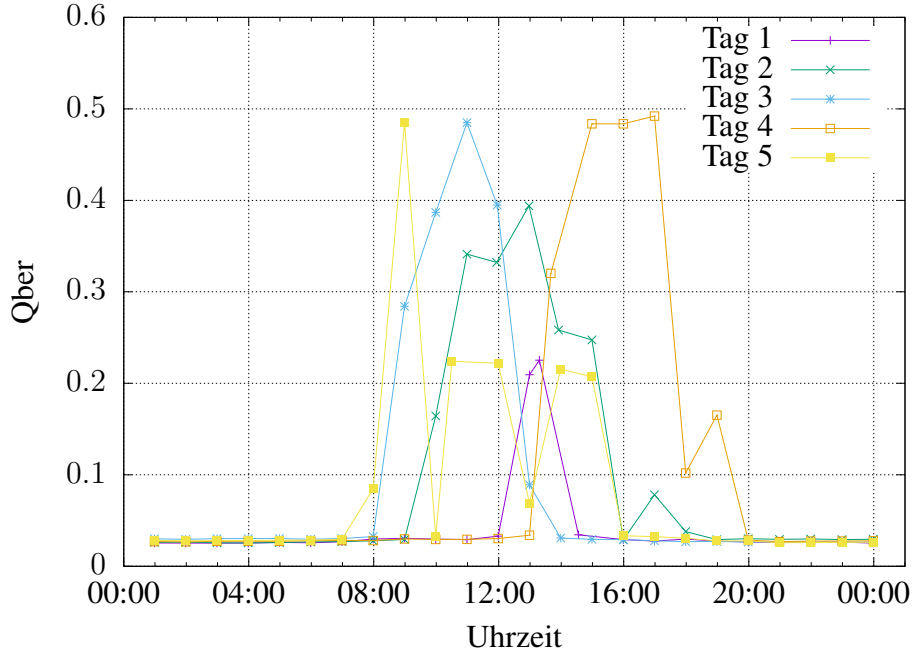

Abbildung 4.14: Tag 1-5 - Qber - Messung 2

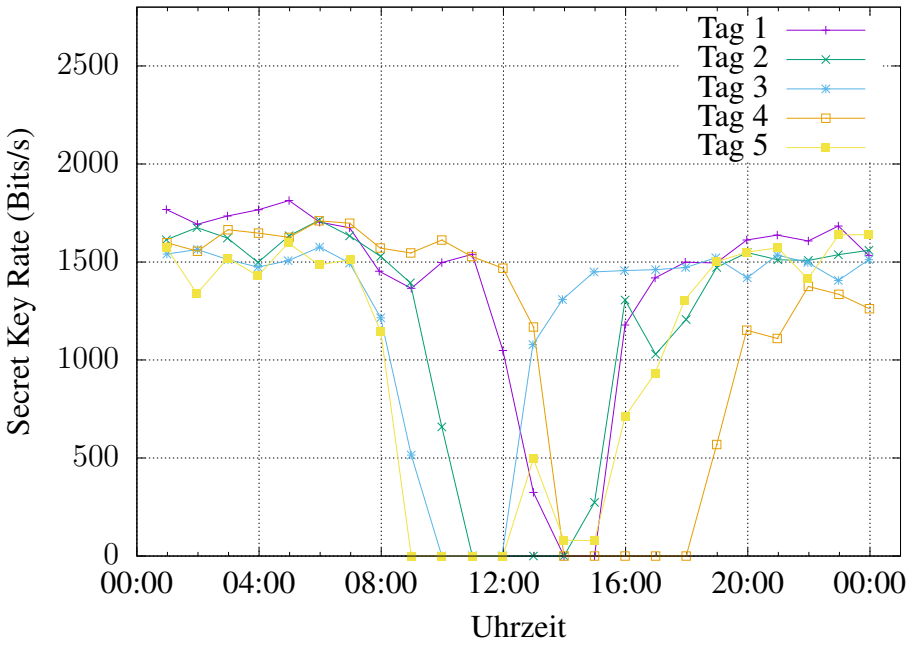

Abbildung 4.15: Tag 1-5 - Secret Key Rate - Messung 2

4.2 Einfluss von Tageslicht

Diese Versuchsreihe sollte die These, dass die Geräte von dem Tageslicht beeinflusst werden, bestätigen und somit die Grundlage für eine mögliche Arbeitsumgebung der Geräte liefern. Weiterhin soll untersucht werden, inwiefern sich die äußeren Einflüsse unter den zur Verfügung stehenden Bedingungen (in einem normalen Büroraum oder Serverraum anstatt in einem Optiklabor) vermeiden lassen und welche Betriebsbedingungen damit zu erreichen sind.
Deswegen wurden die Stationen in dieser Studie wieder über einen längeren Zeitraum laufen gelassen, ohne Änderungen am Versuchsaufsbau vorzunehmen. Die Rahmenbedingungen dieser Messung wurden durch das herunterlassen der Jalousien leicht verändert. Diese mussten zunächst repariert werden, um einen möglichst guten Schutz zur Abdunklung des Raumes zu ermöglichen. Hinzufügend wurde noch eine Abdeckung über die Station Clavis3-B sowie die angeschlossenen Konnektoren gelegt, um die Detektoren nochmals vor dem einfallenden Restlicht zu bewahren. Lediglich die Kabel der Stationen wurden nicht zusätzlich abgedeckt. Der benutzte Attenuator hatte eine Stärke von 10 dB.
Für die anschauliche Darstellung der gemessenen Werte wurden, wie zuvor, die Mittelwerte und Schwankungsbreiten über Zeiträume von jeweils einer Stunde gebildet. Bei dieser Messung wurden für jeden der drei Werte, an jedem Tag, ein Diagramm erstellt. In diesem Unterkapitel wird beispielhaft ein Tag ausgewählt und vorgestellt. Ferner werden die Diagramme, in denen alle Tage verglichen werden, erläutert. Die restlichen Diagramme befinden sich im Anhang.

In dem Diagramm 4.16 ist zu sehen, dass die „Visibility“ während dieser Messung nahezu konstant geblieben ist. Sowohl die Mittelwerte als auch die Standardabweichung, weichen in allen Datenpunkten nicht nennswert voneinander ab. Es ist lediglich ein kleiner negativer Trend zur Mittagszeit zu sehen. Dieser kann durch das restliche, in den Raum eingedrungene, Tageslicht zustande gekommen sein, da die Abdeckung nicht zu 100 Prozent lichtabweisend gewesen ist.
Dieser Trend ist auch in Abbildung 4.17 zu beobachten. In dem Diagramm ist zu sehen, dass die Mittelwerte und die Schwankungsbreite der „Qber“ über den kompletten Zeitraum nahezu konstant sind. Jedoch ist auch hier ein leichter Trend zu erkennen, dass die „Qber“ in der Mittagszeit ansteigt. Dies lässt sich auf den selben Grund, wie bei der „Visibility“ zurückführen.
Die Auswirkungen der Abdeckung auf die „Secret Key Rate“ ist in Abbildung 4.18 zu sehen. Auch der Mittelwert der „Secret Key Rate“ ist in dem gesamten Messintervall annähernd konstant geblieben. Es sind lediglich die immer bestehenden Schwankungen der Datenpunkte vorhanden. Diese kommen durchgängig durch die stetige Schwankung der „Visibility“ und der „Qber“ sowie durch das ständige Nachjustieren der Stationen zustande.

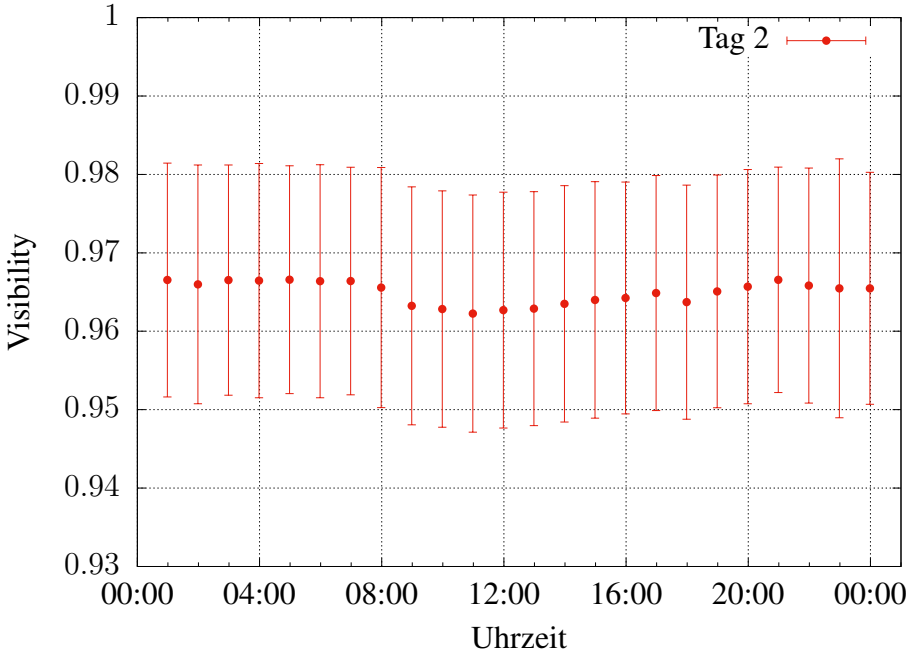

Abbildung 4.16: Tag 2 - Visibility - Abgedeckt

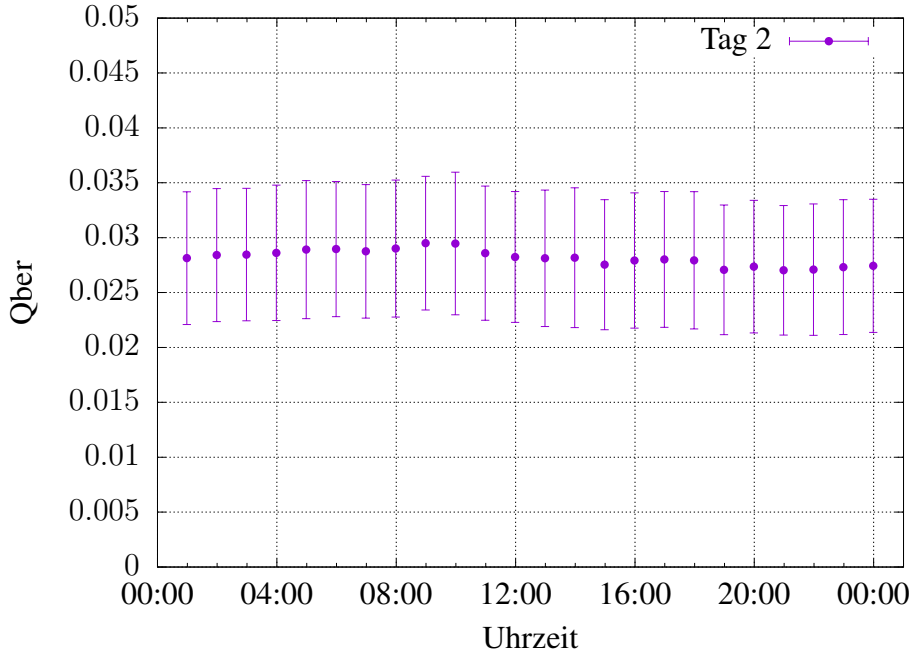

Abbildung 4.17: Tag 2 - Qber - Abgedeckt

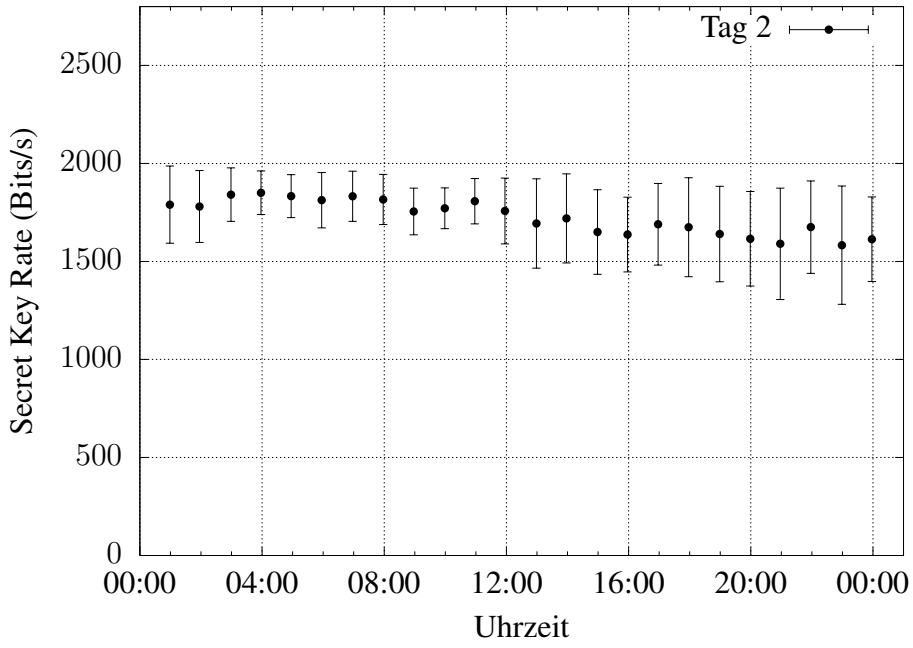

Abbildung 4.18: Tag 2 - Secret Key Rate - Abgedeckt

Das Diagramm 4.19 zeigt, dass der Mittelwert der „Visibility“ an jedem Tag zwischen 96 Prozent und 97 Prozent liegt. Auch ist zu erkennen, dass die „Visibility “ an jedem, außer an dem vierten Tag, zur Mittagszeit abfällt. Die „Qber“ befindet sich im Durchschnitt zwischen 2,5 Prozent und 3 Prozent. Auch hier ist zu erkennen, dass die „Qber“ zur Mittagszeit leicht ansteigt. Dies ist in Abbildung 4.20 zu betrachten. Der Abfall der „Visibility “ ist jedoch deutlicher als der Anstieg der „Qber“.
Die „Secret Key Rate“ ist in dem Diagramm 4.21 zu sehen. An dieser ist deutlich zu erkennen, dass das Abdecken der Geräte und das Verdunkeln des Raumes eine starke Verbesserung der Leistung der Quantenkommunikationsplattform erzielt. Die Mittelwerte der einzelnen Tage befinden sich durchgängig zwischen 1500 Bits/s und 2000 Bits/s.
In Tabelle 4.1 wurden der Mittelwert und die Standardabweichung von allen Werten über den gesamten Zeitraum der Messung gebildet. In dem Zeitraum über vier Tage liegt der Mittelwert der „Visibility“ bei 96,5 Prozent, der Mittelwert der „Qber“ bei 2,8 Prozent und die durchschnittliche „Secret Key Rate“ bei 1770 Bits/s. Diese Werte gilt es dauerhaft sicherzustellen. Sie verschaffen außerdem einen Eindruck, welche Betriebsparameter sich unter realistischen, nicht hochgradig optimierten Bedingungen in einem normalen Büroraum erzielen lassen. Die in der Tabelle 4.1 berechneten Mittelwerte liegen im Bereich der angegebenen Grenzwerte des Supportmitarbeiters von ID Quantique. Die „Qber“ kann laut Angaben des Supportmitarbeiters auf bis zu 2 Prozent sinken. Die „Visibility“ kann laut Angaben auf bis zu 98 Prozent ansteigen. Des Weiteren soll die „Secret Key Rate “ bei über 1400 Bits/s liegen. Diese Aussage kann auch bestätigt werden, da der Mittlerwet der „Secret Key Rate “ über den gesamten Zeitraum der Messung bei 1770.404 Bits/s liegt.

Die Auswertung dieser Versuche ergibt erste Erkenntnisse für eine mögliche Arbeits- und Verwendungsumgebung der Stationen. Die Geräte sollten in einem abgedunkelten Raum verwendet werden. Aus diesem Grund gilt es der Frage nachzugehen, ob die Geräte auch von künstlichem Licht beeinflusst werden. Werden sie dadurch nicht beeinflusst, so können sie in normalen Serverräumen verwendet werden.

Tabelle 4.1: Mittelwert und Standardabweichung der Datenpunkte über alle gemessenen Tage dieser Messreihe

	Mittelwert μ	Standardabweichung σ
Visibility	0.965	0.015
Qber	0.028	0.006
Secret Key Rate	1770.404	851.415

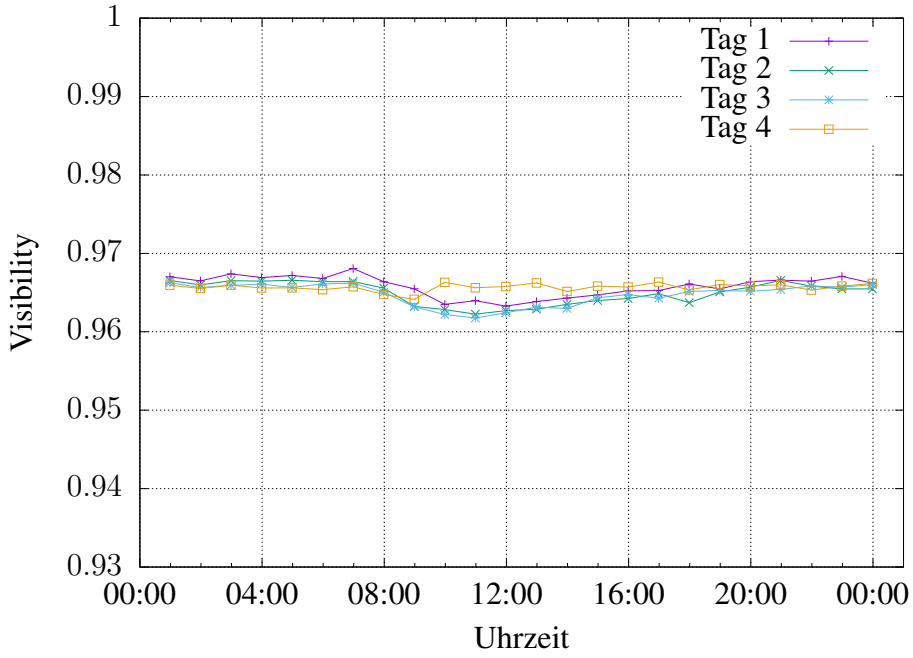

Abbildung 4.19: Tag 1-4 - Visibility - Abgedeckt

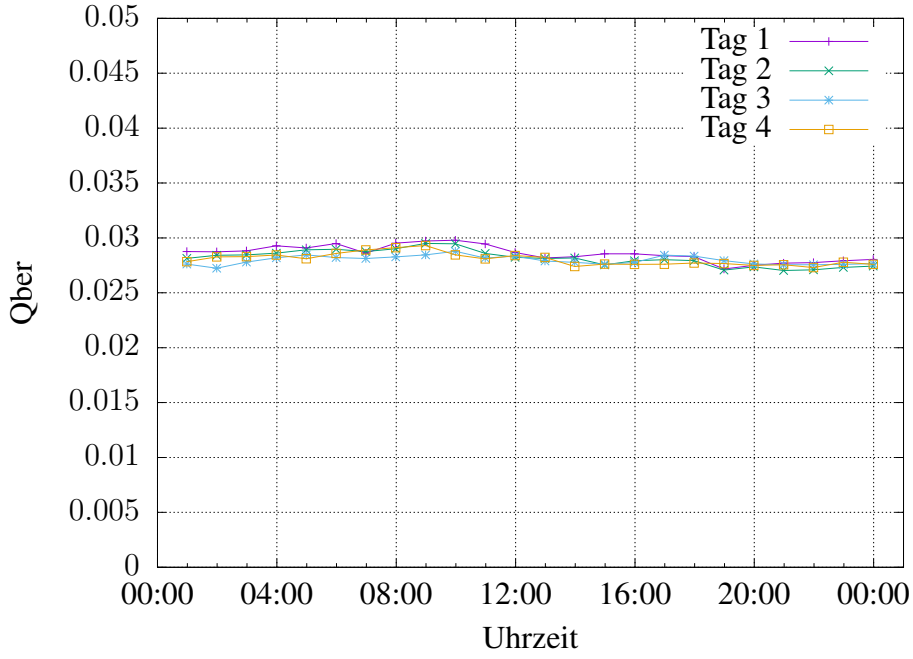

Abbildung 4.20: Tag 1-4 - Qber - Abgedeckt

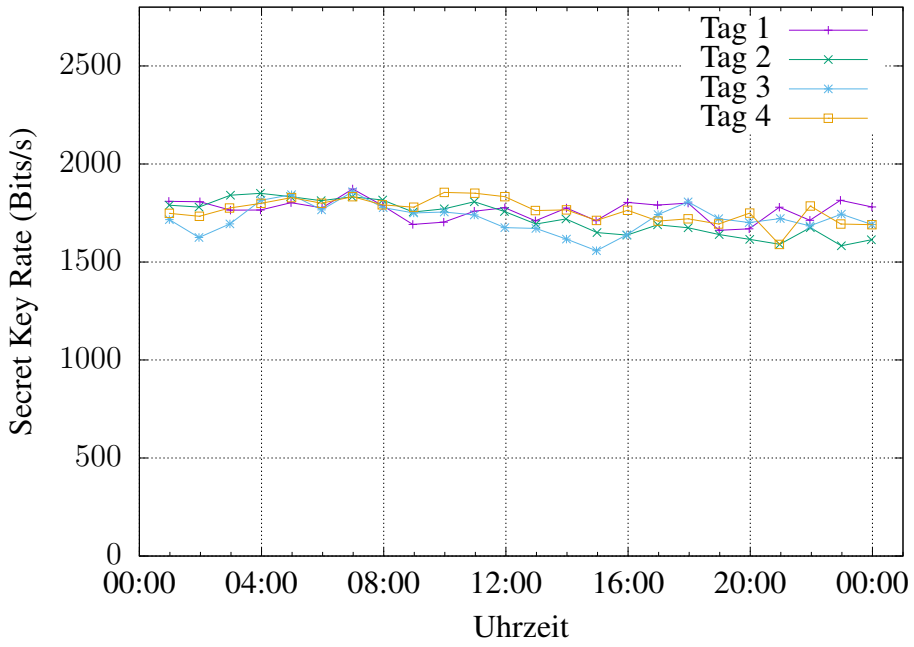

Abbildung 4.21: Tag 1-4 - Secret Key Rate - Abgedeckt

4.3 Einfluss von künstlichem Licht

Die zuvor gewonnene Erkenntnis, dass das Tageslicht einen Einfluss auf die Detektoren und somit die gemessenen Daten hat, führt zu der Frage, ob auch künstlich erzeugtes Licht - durch zum Beispiel eine Deckenlampe oder Bildschirme - einen Einfluss auf die Quantenschlüsselverteilungsplattform hat. Dies ist für den Standort der Stationen wichtig, damit diese nicht von dem künstlichem Licht am Platzierungsort, beispielsweise in einem Serverraum, beeinflusst werden.
Um den Einfluss von Tageslicht komplett ausschließen zu können, wurden die Stationen in einem verdunkelten Raum in der Nacht laufen gelassen und das Deckenlicht wurde eingeschaltet. In einer anderen Messung wurde auch das Deckenlicht in der Nacht ausgeschaltet. Der benutzte Attenuator besaß eine optische Dämpfung von 10 dB.
Zum Auswerten der gemessenen Daten wurden der Mittelwert und die Schwankungsbreite über einen Zeitraum von drei Stunden gebildet und in einem Diagramm gegenübergestellt. Der gewählte Zeitraum war von 00:00 Uhr bis 03:00 Uhr, somit war der Einfluss von Tageslicht auszuschließen.

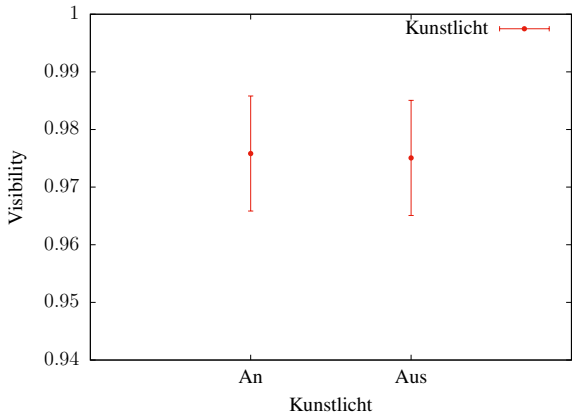

Abbildung 4.22: Visibility - Kunstlicht

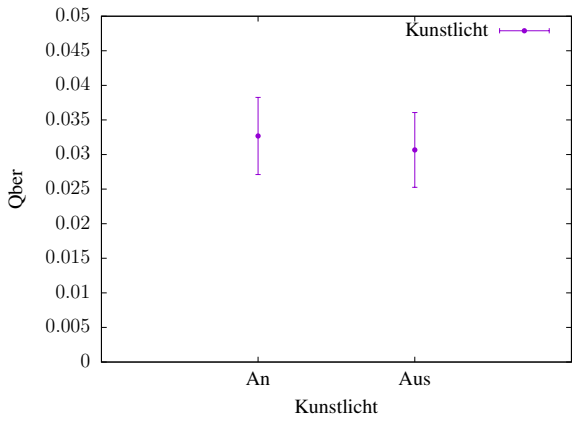

Abbildung 4.23: Qber - Kunstlicht

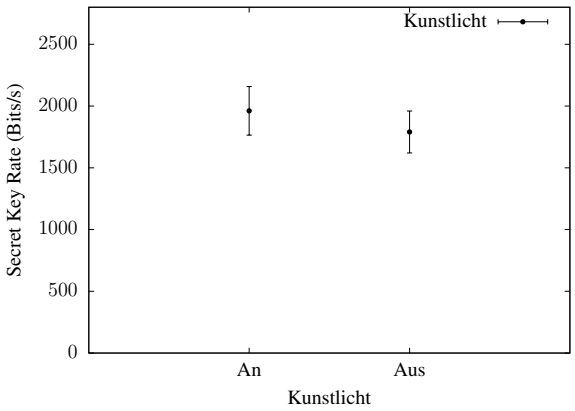

Abbildung 4.24: Secret Key Rate - Kunstlicht

Aus dieser Messreihe geht hervor, dass künstliches Licht keinen signifikanten Einfluss auf die Quantenverschlüsselungsplattform hat. In den Diagrammen 4.22, 4.23 und 4.24 ist sogar zu sehen, dass die Parameter der Geräte bei eingeschaltetem und ausgeschaltetem Licht keinen signifikaten Unterschied in den Werten aufweisen. Dieser Unterschied ist aber zu vernachlässigen, weil die Stationen sich selbst dauerhaft nachjustieren und es dadurch zu kleinen, zufälligen Abweichungen im Verhalten kommen kann. Außerdem kann es durch die Vibration der Geräte zu leichten Veränderungen der Ausrichtung des Glasfaserkabels des Quantenkanals kommen. Jegliche Änderungen der Ausrichtung können den Wert der Datenpunkte ebenfalls beeinflussen, da der Quantenkanal sehr empfindlich ist.

Diese Erkenntnis führt zu weiteren Informationen über die Rahmenbedigungen der Arbeits- und Verwendungsumgebung der Geräte. Die Geräte können problemlos in einem, von der Sonne abgeschotteten Raum in Betrieb genommen werden. Normales künstliches Licht von beispielsweise Arbeits- oder Deckenlampen hat keine deutlichen Auswirkungen auf die Funktionalität der Stationen.

4.4 Auswirkungen des Eavesdropping-Simulators

Der Eavesdropping-Simulator wird zwischen den beiden Stationen angeschlossen und versucht, Informationen über den Schlüssel, der zu dem Zeitpunkt erzeugt wird, zu erhalten und fügt dabei der Übertragung unweigerlich Rauschen hinzu beziehungsweise führt er das ursprüngliche Signal zeitverzögert in die Übertragung zurück. Des Weiteren hat er eine optische Dämpfung von 3 dB. Zudem besitzt der Eavesdroppin-Simulator einen verstellbaren Regler, mit dem man die Intensität des Rauschens einstellen kann. Bei dieser Messreihe wurde die Skala in Intervallen von 5 Einheiten erhöht, jedoch sind keine genaue Angaben über die Bedeutung der Skala vorhanden. Je höher die Skala, desto höher das Rauschen. Je höher das Rauschen, desto mehr Informationen hat der Eavesdropping-Simulator erhalten.
Ziel dieses Versuches war es, Aussagen über die Auswirkungen eines Angreifers, der in diesem Fall durch den Eavesdropping-Simulator simuliert wird, treffen zu können. Genauer gesagt: Wie verhalten sich die Geräte mit zunehmender Störung durch den Eavesdropping-Simulator? Auch galt es zu klären, welche Auswirkungen ein Angriff auf die „Qber“ und die „Visibility“ hat und ab wann man einen Angriff erkennen kann.
Dazu wurde der Quantenkanal von der Station Clavis3-A an den Eingang des Eavedropping-Simulators und der Quantenkanal des Ausgang des Eavesdropping-Simulators an den Eingang der Station Clavis3-B angeschlossen. Außerdem wurde zusätzlich ein Attenuator mit einer optischen Dämpfung von 10 dB verwendet.
Der Mittelwert und die Schwankungsbreite der gemessenen Werte wurden über den Zeitraum gemessenen berechnet. Diese wurden jeweils mit den verschiedenen Einstellungswerten des Eavedropping-Simulators in einem Diagramm zusammengefasst.

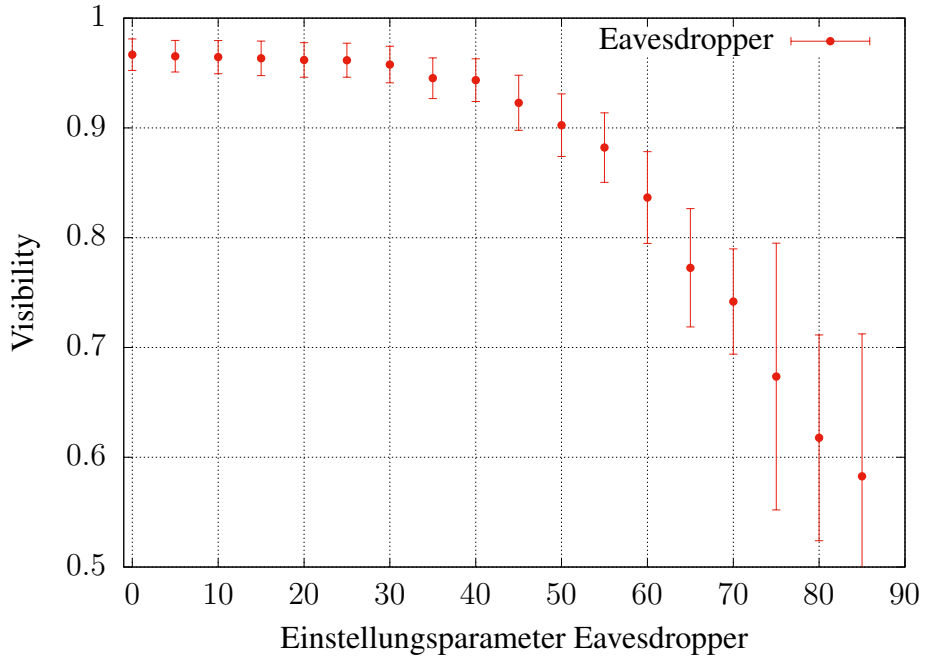

Abbildung 4.25: Visibility - Eve

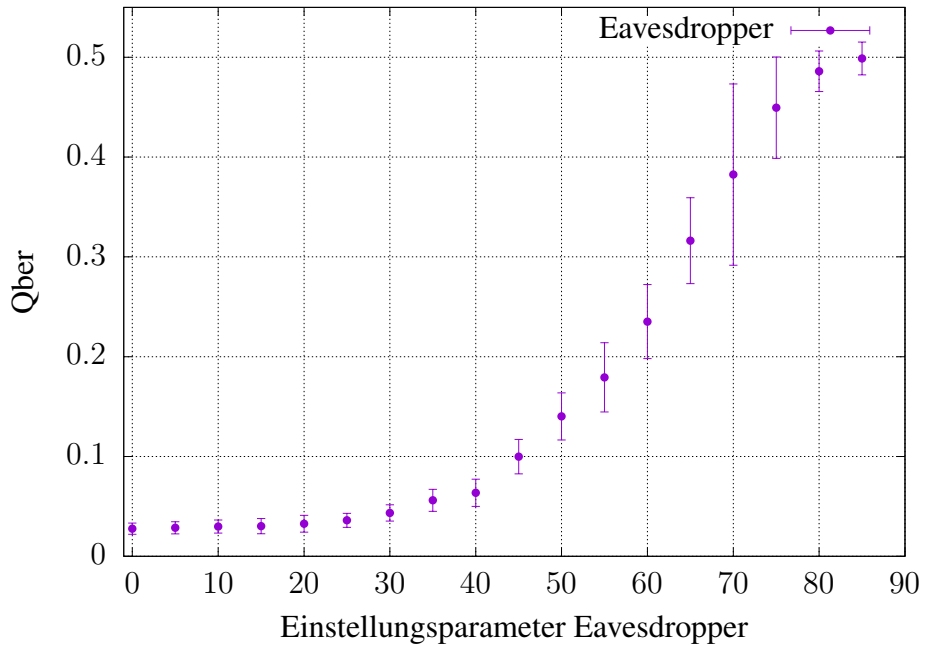

Abbildung 4.26: Qber - Eve

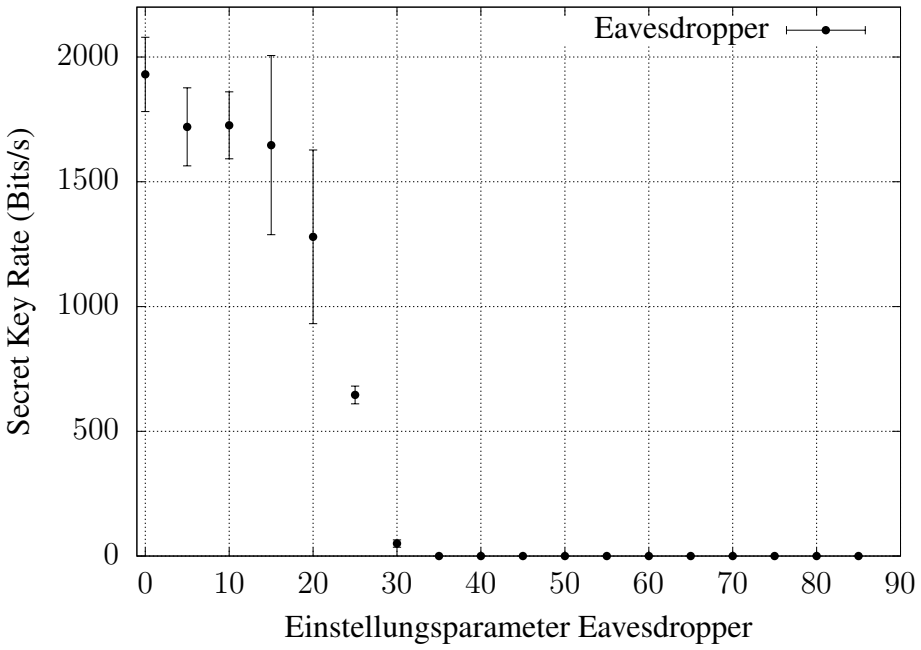

Abbildung 4.27: Secret Key Rate - Eve

In den Abbildungen 4.25 und 4.26 ist grundsätzlich zu erkennen, dass die Werte der „Visibilty“ absinken und die Werte der „Qber“ ansteigen, je höher die Skala des Eavedropping-Simulators eingestellt ist.
Anfangs, bei Werten für den Einstellungsparameter des Eavesdropping-Simulators im Bereich von 0 bis 35, ist bei der Erhöhung der Skala kein nennenswerter Unterschied zwischen den einzelnen Einstellungen zu betrachten. Jedoch ist der Trend der Verschlechterung der Werte zu sehen. Wird jedoch der Sprung von 0 auf 35 betrachtet, ist die Verschlechterung deutlich erkennbar. Die Verschlechterung der „Secret Key Rate“, die in Abbildung 4.27 zu erkennen ist, ist jedoch deutlich sichtbar. Die Produktion der geheimen Schlüssel sinkt in diesem Zeitraum radikal ab.
Ab der Einstellungsskala 40 des Eavedropping-Simulators ist es den Geräten nicht mehr möglich, geheime Schlüssel zu produzieren. Dabei liegt der Mittelwert der „Visibility“ bei 94,5 Prozent und der Mittelwert der „Qber“ bei 5,6 Prozent. Dies stimmt mit den von dem Supportmitarbeiter von ID Quantique angegebenen Werten überein. Laut des Mitarbeiters liegt der Höchstwert der „Qber“, bei dem noch geheime Schlüssel generiert werden, bei circa 4,5 Prozent und der Mindestwert der „Visibility“ bei circa 95 Prozent. Ab diesem Punkt ist auch der Anstieg der „Qber“ und der Abfall der „Visibility“, in jedem Intervall, deutlich zu sehen. Obendrein erhöht sich die Standardabweichung der „Visibility“ drastisch, vor allem bei dem Sprung von 70 auf 75.
Die Erhöhung der „Qber“ lässt sich auf das Hinzufügen des Rauschens des Eavedropping-Simulators zurückführen. Je höher die Quantität des Rauschens, welches der Übertragung hinzugefügt wird, desto höher ist die „Qber“. Die Reaktion der Quantenschlüsselverteilungsplattform auf den Angriff, ist die Erhöhung der Datenschutz-Verstärkung. Durch die Erhöhung der Datenschutz-Verstärkung kommt es zu niedrigeren Schlüsselra-

ten. Auch dauert die Datenpunkterzeugung ´der „Secret Key Rate“ länger, da der Buffer, der vor jedem Datenpunkt aufgebaut wird, nun länger zum Erreichen des Maximums benötigt. Ohne Eavesdropping-Simulator wird circa alle 2 Minuten ein Datenpunkt erzeugt, bei der Einstellung 35 auf der Skala, sind es circa 15 Minuten.

Die Quantenschlüsselverteilungsplattform kann mit Hife des „Post-Processing“ bis zu einem bestimmten Punkt trotz eines Angriffs noch Schlüssel erzeugen. Jedoch ist die Folge eines Angriffs, dass die Schlüsselrate sinkt.
Ob ein „Lauschangriff“ durch den Eavesdropping-Simulator auf die Quantenschlüsselverteilungsplattform vorliegt, ist durch verschiedene Indikatoren erkennbar. Zum einen steigt die Generierungszeit der Datenpunkte der „Secret Key Rate“. Dementsprechend nimmt die Anzahl an Bits/s, des produzierten geheimen Schlüsselmaterials, ab. Ein anderer Indikator eines Angriffes ist die Zunahme der „Qber“. Diese steigt an, sobald der Übertragung durch einen Angriff Rauschen hinzugefügt wird. Einhergehend damit sinkt die „Visbility“ mit ansteigendem Rauschen. Sobald eine Zeit lang keine geheimen Schlüssel mehr produziert werden können, starten sich die Stationen neu. Auch dies kann ein möglicher Indikator eines Lauschangriffs sein.

4.5 Auswirkungen verschiedener optischer Verluste

Ein Ziel dieser Studie war es, die optische Dämpfung herauszufinden, bei der die optimale Schlüsselrate und die bestmögliche Stabilität gewährleistet sind. Ferner war ein Ziel, die maximale optische Dämpfung zu bestimmen, bei der noch ein Schlüsselaustausch möglich ist.
Mit Hilfe des Ergebnisses des ersten Ziels lässt sich bestimmen, wie die optische Dämpfung der Geräte, nach Verlegung an zwei verschiedene Standorte, gewählt werden sollte, da sich die gesamte optische Dämpfung aus der Dämpfung der Glasfaserstrecke, sowie aus der Dämpfung eines noch zusätzlich eingefügten Attenuators zusammensetzt.
Dazu wurden die Geräte abgedeckt und in einem verdunkelten Raum in Betrieb genommen. Nach gewissen Zeitabständen wurde der Attenuator gewechselt und die Stationen wurden neu gestartet. Über einen Zeitraum mit konstanten Bedingungen wurden der Mittelwert und die Schwankungsbreite berechnet. Die Zeiträume sind so gewählt worden, dass bei jeder der verschiedenen optischen Dämpfungen zwischen 12 und 15 Datenpunkte der „Secret Key Rate“ erzeugt wurden, sodass ein sinnvoller Mittelwert über diese Punkte gebildet werden konnte.
Die berechneten Werte sind in einem Diagramm zusammengefasst und gegenübergestellt worden. Der x-Achsen-Fehlerbalken ist eine Besonderheit an den Diagrammen. Dieser ensteht aufgrund der Messunsicherheit der verschiedenen Attenuatoren. Um jede abgebildete optische Dämpfung testen zu können, mussten zuweilen zwei verschiedene Attenuatoren kombiniert werden. In diesem Fall wurde auch die Messunsicherheit der optischen Dämpfung der Attenuatoren addiert. Eine Tabelle der benutzten Attenuatoren, samt der Stückelung und der Messunsicherheit, findet sich in Anhang D.1.
Die niedere Grenze der optischen Dämpfung wurde bei 4 dB gewählt. Der Grund dafür ist die Mindestdämpfung der Strecke des Einsatzbereiches. Sobald die Geräte an den verschiedenen Standorten stehen, ist eine Mindestdämpfung von circa 4 dB allein durch die Strecke des Glasfaserkabels zwischen den Standorten gewährleistet. Zudem gibt der Hersteller ID Quantique eine Mindestdämpfung von 10 dB für die Geräte an, weswegen nicht klar ist, wie die Geräte bei zu niedriger optischer Dämpfung reagieren. Um die Geräte zu schonen und vorsichtig mit diesen umzugehen, wurde keine geringere optische Dämpfung als 4 dB getestet.

In der Abbildung 4.28 ist ein Abfall der „Visibility“ mit steigender Attenuation zu erkennen. Der Grund dafür liegt in der Detektion der einzelnen Photonen. Je mehr Photonen korrekt detektiert werden, desto höher ist der Wert der „Visibility“. Durch die geringere optische Dämpfung können die Photonen besser detektiert werden und es kommt zu weniger Fehlmessungen, da die Photonen deutlicher detetktiert werden können. Wird ein höherer Anteil der Photonen in den entsprechenden Zeitintervallen detektiert, steigt die „Visibility“. Der Unterschied zwischen 4 dB und 5 dB ist entweder durch Übersättigung des Detektors, durch die Messungenauigkeiten der Attenuatoren oder durch die Neukalibrierung der Quantenschlüsselverteilungsplattform zu erklären.

Ist der Detektor übersättigt, kann er nicht mehr alle „Visibility“ steigernden Photonen detektieren. Somit sinkt die „Visibility“. Weiterhin sind die Messungenauigkeiten der Attenuatoren ein möglicher Grund. Durch das Zusammenstecken verschiedener Attenuatoren ist es möglich, dass bei der Messung mit einer optischen Dämpfung von 4 dB eigentlich eine optische Dämpfung von 5 dB vorlag. Bei der Messung mit einer optischen Dämpfung von 5 dB ist es möglich, dass die tatsächliche optische Dämpfung nur 4,5 dB betrug.
In dem Diagramm 4.29 ist das Verhalten der „Qber“ bei verschiedenen optischen Dämpfungen dargstellt. In der Grafik ist bis 12 dB ein stetiger Abfall der „Qber“ zu betrachten. Ab einer optischen Dämpfung von 12 dB steigt diese jedoch wieder an.
Es gibt zwei verschiedene Gründe für den Anstieg der „Qber“ bei niedriger optischer Dämpfung. Ein möglicher Grund ist der Jitter, also das zeitliche Taktzittern bei der Übertragung, welches zu Genauigkeitsschwankungen im Übertragungstakt führt. Der Jitter beeinflusst auch die Phasenlage. Bei höheren Detektionsraten, durch niedrigere optische Dämpfung, erhöht sich auch der Jitter. Die Folge der Erhöhung des Jitters ist die Erhöhung der Fehlerrate.
Das Coherent One-Way-Protokoll benutzt Photonenpulse. Sobald eines der Photonen detektiert wird, gilt der ganze Photonenpuls als detektiert. Es ist auch möglich, kein Photon des Photonenpulses zu detektieren. Bei niedriger optischer Dämpfung kommen mehr Photonen beim Detektor an. Durch das Rauschen des Lasers werden auch zufällig Photonen erzeugt. Diese unerwünscht erzeugten Photonen werden bei einer Mindestdämpfung von 10 dB nur sehr selten detektiert. Ist die optische Dämpfung jedoch niedriger, ist es wahrscheinlicher, dass die von dem Rauschen erzeugten Photonen detektiert werden, während die Detektionsrate der Photonenpulse sich aufgrund des vorher erwähnten Effekts nicht in gleichem Maße verbessert. Somit kommt es zu einer höheren Fehlerrate in der Detektion der Photonen, was einen Anstieg der „Qber“ zur Folge hat.
In der Abbildung 4.30 ist die Veränderung der „Secret Key Rate“ bei unterschiedlicher optischen Dämpfung zu sehen. Der Anstieg der „Visibility“ bei niedrigerer optischer Dämpfung erklärt den Anstieg der „Secret Key Rate“ bei niedriger optischer Dämpfung. Demnach ist in der Abbildung zu erkennen, dass die Schwankungsbreite der Produktionsrate von geheimen Schlüsseln bei niedriger optischer Dämpfung sehr groß und zufällig ist. Dies ist bei 5 dB im Vergleich zu 6 dB und 7 dB zu erkennen. Obwohl die optische Dämpfung reduziert wurde, ist die Standardabweichung geringer geworden.

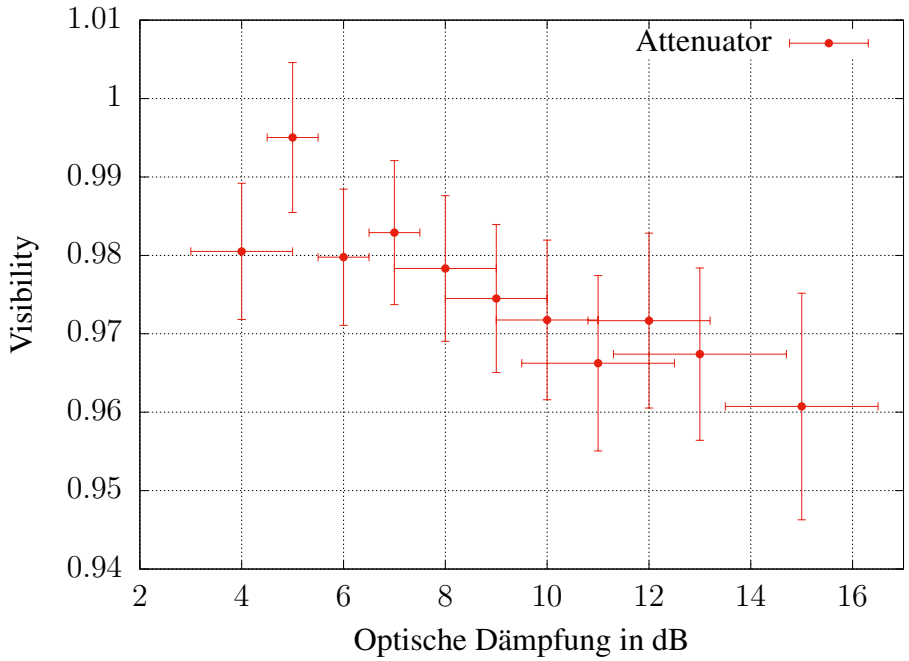

Abbildung 4.28: Visibility - Attenuatoren

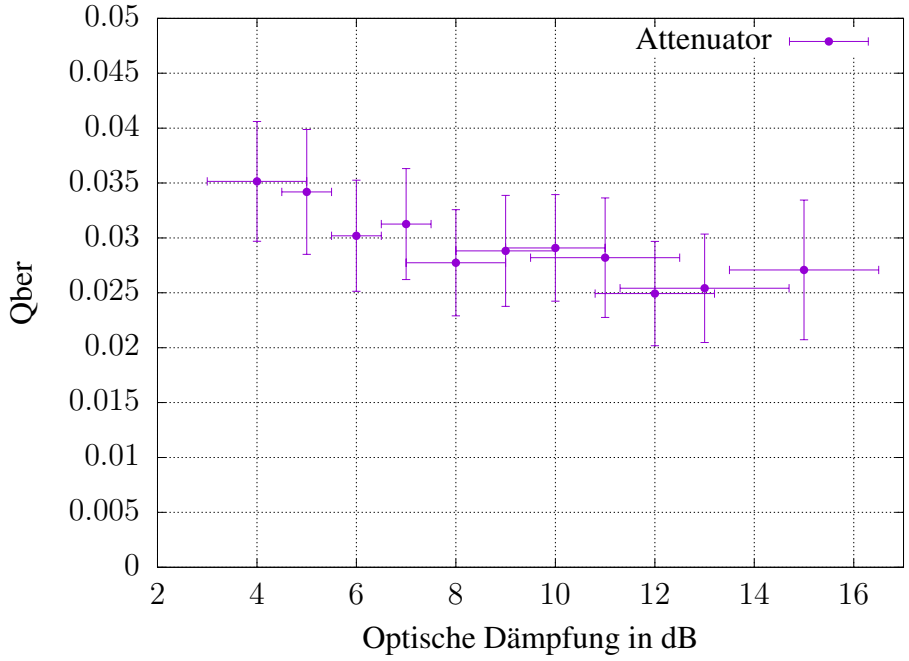

Abbildung 4.29: Qber - Attenuatoren

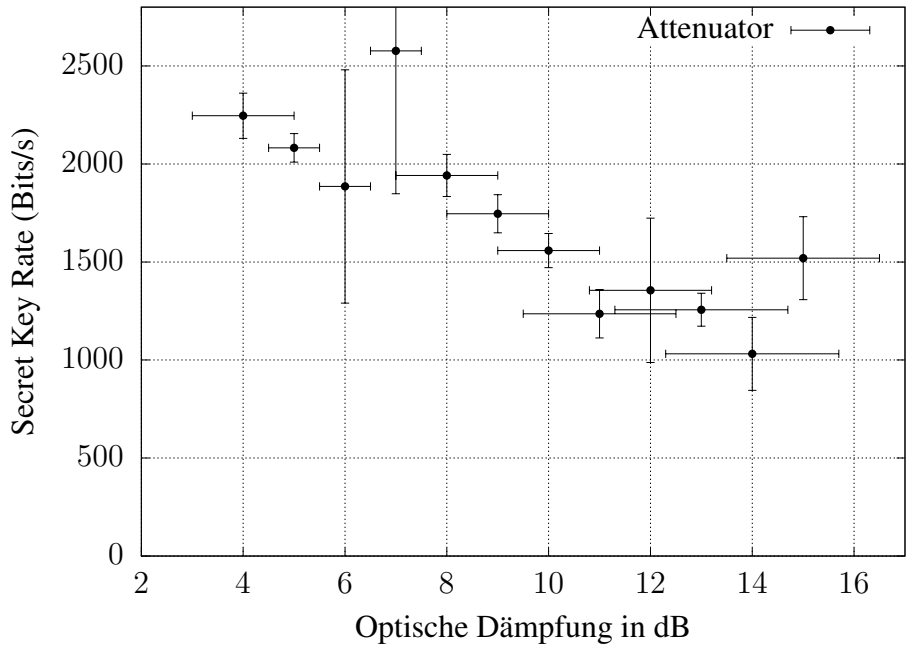

Abbildung 4.30: Secret Key Rate - Attenuatoren

Die Quantenverschlüsselungsplattform ist bis zu einer optischen Dämpfung von 15 dB in der Lage geheime Schlüssel zu produzieren. Somit liegt diese über der vom Hersteller angegebenen optischen Dämpfung von 12 dB. ID Quantique garantiert, dass die Geräte bei einer optischen Dämpfung von 12 dB auf jeden Fall funtkionieren. Dieses ermöglicht die Geräte über eine größere Reichweite als 60 km zu betreiben, wenn man mit einem optischen Verlust von 0,2 dB pro Kilometer rechnet. Eine Entfernung von 60 km entspricht einer optischen Dämpfung von 12 dB. So liegt die Begrenzung der Reichweite bei 75 km. Dies entspricht dann 15 dB an optischem Verlust.
Der beste Betriebsmodus der Geräte, in Bezug auf die Mittelwerte der verschiedenen Größen, liegt bei einer optischen Dämpfung zwischen 8 dB und 10 dB. In diesem Bereich ist die „Visibility“ zwischen 97 Prozent und 98 Prozent. Des Weiteren befindet sich die „Qber“ in einem Wertebereich zwischen 2,5 Prozent und 3 Prozent. Zwischen 8 dB und 10 dB liegt die „Secret Key Rate“ zwischen 1500 Bits/s und 1900 Bits/s. Diese Werte befinden sich in dem von dem Supportmitarbeiter angegebenen möglichen Wertebereich. Die „Visibility“ erreicht circa die obere angegebene Grenze. Die „Secret Key Rate“ ist höher als die von dem Hersteller im Mittelwert garantierten 1400 Bits/s. Lediglich die „Qber“ ist im Vergleich zu den bestmöglich zu erreichenden Werten leicht erhöht. Die von dem Supportmitarbeiter angegebenen Werte finden sich in Unterkapitel 3.3. Bei diesen optischen Dämpfungen ist die Standardabweichung der „Secret Key Rate“ sehr gering. Somit erhält man eine konstant und stabil hohe Produktionsrate von geheimen Schlüsseln. Eine stabile und verlässliche „Secret Key Rate“ ist für die Benutzung der Quantenverschlüsselungsplattform von großem Wert.

Kapitel 5

Fazit und Ausblick

Das letzte Kapitel der Arbeit dient dazu, die durchgeführten Versuchsreihen und die wichtigsten Erkenntnisse zusammenzufassen. Überdies wird die „Secret Key Rate“, in anderer Darstellungsform, mit dem von dem Supportmitarbeiter angegebenden Wert gegenübergestellt. Am Ende wird ein Ausblick auf eine mögliche Fortsetzung der Arbeit gegeben.

5.1 Fazit

Zunächst wurden im ersten Kapitel Begriffsdefinitionen vorgestellt, um ein grundlegendes Wissen über den Quantenschlüsselaustausch zu schaffen. Weiterhin wurden im zweiten Kapitel zwei verschiedene Protokolle vorgestellt, die für den Quantenschlüsselaustausch genutzt werden. In dem darauf folgenden dritten Kapitel wurde das Projekt MuQuaNet, welches den thematischen Rahmen bietet, in dem diese Masterarbeit entstanden ist präsentiert. Zudem wurden auch die Quantenschlüsselverteilungsplattform Clavis[3] und die mitgelieferte Steuersoftware beschrieben. Der Versuchsaufbau sowie die Methodik vorgestellt wurden vorgestellt. Als letzter Punkt des Kapitels wurde die Darstellung der gewonnenen Daten durch die Versuchsreihen charakterisiert. In dem vorletzten, vierten Kapitel der Arbeit wurden die verschiedenen Versuchsreihen beschrieben und ausgewertet. Weiter wurden Erkenntnisse zu den Rahmenbedingungen der Nutzung der Quantenschlüsselverteilungsplattform gewonnen.
Diese Arbeit hat durch verschiedene Versuchsreihen die Quantenschlüsselverteilungsplattform Clavis[3] untersucht und Erkenntnisse über die Rahmenbedingungen für den Einsatz der Geräte gewonnen. Dabei lag der Fokus der Untersuchungen auf der Stabilität der Geräte, den Auswirkungen des Eavedropping-Simulators sowie den Auswirkungen verschiedener optischer Dämpfungen in Bezug auf die „Qber“, die „Visibility“ und die „Secret Key Rate“.

Aus der Versuchsreihe über die Stabilität der Geräte im Zeitverlauf ging hervor, dass das Tageslicht eine große Störquelle der Quantenschlüsselverteilungsplattform ist. Die Geräte waren teilweise nicht in der Lage, Schlüsselmaterial zu erzeugen. Dies lag an dem Anstieg der „Qber“ und dem Abfall der „Visibility“. Mit einer zweiten Studie über die Stabilität der Geräte wurden andere Fehlerquellen ausgeschlossen, da verschiedene Komponenten ausgetauscht wurden, die Fehler jedoch gleich blieben.
Daraufhin wurde eine weitere Stabilitätsstudie durchgeführt, jedoch wurden das Labor verdunkelt und die Geräte zusätzlich abgedeckt. Folglich liefen die Geräte, ohne einen Neustart, über einen Zeitraum von vier Tagen stabil. Die Mittelwerte der „Qber“ und der „Visibilty“ hielten sich dabei im Rahmen des von Hersteller angegebenen Wertebereiches. Auch der Mittelwert der „Secret Key Rate“ lag dauerhaft über 1400 Bits/s. Anhand dieser Messung wurde die Abbildung 5.1 erstellt. In dem Diagramm ist zu erkennen, wie viel Prozent der Datenpunkte gleich oder über einem bestimmten Wert der „Secret Key Rate“ liegen. Der vom Hersteller angegebene Wert der „Secret Key Rate“, welcher bei einer „Qber“ zwischen 2 Prozent und 4,5 Prozent und einer „Visibility“ zwischen 95 Prozent und 98 Prozent dauerhaft erreicht werden soll, liegt bei mindestens 1400 Bits/s. Aus dem Diagramm 5.1 geht hervor, dass 93 Prozent aller Datenpunkte der „Secret Key Rate“ mindestens einen Wert von 1400 Bit/s haben. Wird definiert, dass unter stabiler Schlüsselerzeugung verstanden wird, dass der prozentuale Anteil der Datenpunkte der „Secret Key Rate“ zwischen 90 Prozent und 95 Prozent liegen muss, so erzeugt das System stabil 1400 Bit/s an geheimem Schlüsselmaterial. Aus der Tabelle 4.1 geht hervor, dass der Mittelwert der „Secret Key Rate“ über den gesamten Messzeitraum über 1770 Bits/s liegt. Dieser Wert ist höher als der vom Hersteller angegebene. Dementsprechend kann gefolgert werden, dass unter den normalen Betriebsbedingungen in einem verdunkelten Büroraum sehr zufriedenstellende und auch über die Zeit hinweg stabile Resultate für die Schlüsselrate erzielt werden können.
Aufgrund der Ergebnisse der Stabilitätsstudien ergab sich die Frage, welche Bedingungen der Standort beziehungsweise der Raum, in dem die Geräte in Betrieb genommen werden, berücksichtigt werden muss. Aus diesem Grund wurde der Einfluss von künstlichem Licht auf die Quantenschlüsselverteilungsplattform untersucht. Das Ergebnis der Messung ergab, dass künstliches Licht keinen Einfluss auf die Geräte hat. Daraus ergab sich, dass die Geräte problemlos in einem von der Sonne abgeschotteten Raum, zum Beispiel in einem Serverraum, in Betrieb genommen werden können. Normales künstliches Licht von beispielsweise Arbeits- oder Deckenlampen hat keine deutlichen Auswirkungen auf die Funktionalität der Stationen.
Bei einem simulierten Angriff mit Hilfe des Eavesdropping-Simulators steigt die „Qber“ mit Erhöhung der Einstellungen auf der Skala des Eavesdropping-Simulators an. Die „Visibility“ sinkt genau wie die „Secret Key Rate“ dabei ab. Trotz eines Lauschangriffes durch den Eavesdropping-Simulator ist die Quantenschlüsselverteilungsplattform, durch das „Post-Processing“, bis zu einem bestimmten Wert auf der Skala des Eavesdropping-Simulators in der Lage, geheime Schlüssel zu produzieren.
Bei der Versuchsreihe über die verschiedenen optischen Dämpfungen galt es die Forschungsfragen zu klären, bis zu welcher optischen Dämpfung die Geräte in der Lage sind, geheime Schlüssel zu produzieren und bei welcher optischen Dämpfung eine best-

mögliche und möglichst hohe, stabile Schlüsselgenerierung möglich ist. Dies galt es aufgrund der geplanten Verlegung der Geräte an verschiedene Standorte zu überprüfen. Die Glasfaserstrecke zwischen den Standorten besitzt auch eine optische Dämpfung, weshalb es herauszufinden galt, welche optische Dämpfung der Station Clavis3-B, mit Hilfe eines Attenuators, hinzugefügt werden muss, um die optimale optische Dämpfung zu erreichen. Das Ergebnis der Auswertung der Messreihe ergibt, dass die optimale optische Dämpfung zwischen 8 dB und 10 dB liegt. Beträgt also die optische Dämpfung der Dark Fiber Strecke zwischen CODE und UniBw-Campus 4 dB, lässt sich aus dem Ergebnis die Empfehlung ableiten, einen zusätzlichen Attenuator mit 4-6 dB zu verwenden.

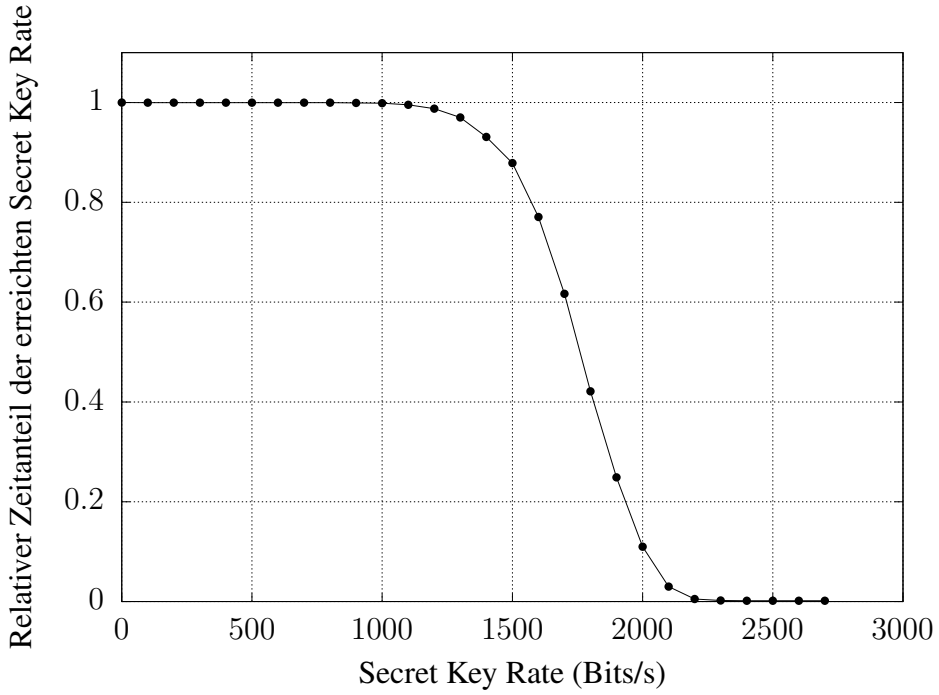

Abbildung 5.1: Relativer Zeitanteil der erreichten „Secret Key Rate“

5.2 Ausblick

Eine weitere interessante Erkenntnis wäre, die Geräte nach ihrer Up-/Downtime zu bewerten. Also der zeitliche Anteil, wie lange ein gewisser Wert der „Secret Key Rate“ erreicht wird.
Zusätzlich wäre eine weitere mögliche Fortsetzung dieser Arbeit das Testen des „Dense Wavelength Division Multiplexings“ in Bezug auf die Quantenschlüsselverteilungsplattform Clavis[3]. Bei dem „Dense Wavelength Division Multiplexings“ handelt es sich um eine Technologie, mit derer Datensignale aus verschiedenen Quellen zusammengefügt werden. Dabei bleibt die vollständige Trennung der Datenströme vorhanden. Mit Hilfe dieser Technologie ist es möglich, Datensignal aus verschiedenen Quellen mit einem einzigen Glasfaserkabel zu versenden.
Dies ist für das Projekt MuQuaNet von großem Nutzen, da zwischen zwei Standorten

nur zwei benutzbare Glasfaserkabel vorhanden sind. Eines der beiden ist für den Quantenkanal reserviert. Auf dem anderen Glasfaserkabel soll der klassische Kanal mit dem verschlüsselten Datenverkehr und Keymanagement-Verkehr zusammengefasst werden. Diese Technologie sollte im Labor getestet werden, bevor die Geräte an verschiedene Standorte verlegt werden. Ein schematischer Versuchsaufbau mit dieser Technologie ist in Anhang E zu sehen.
Auf der ersten Fortsetzung aufbauend, ist es möglich die Geräte an verschiedene Standorte zu verlegen und in Betrieb zu nehmen. Dort gilt es zu überprüfen, ob die Quantenschlüsselverteilungsplattform stabil und konstant läuft. Dabei ist es wichtig, die Fehlerquellen zu minimieren und die in dieser Arbeit herausgearbeiteten Punkte zu beachten. Unter Beachtung der herausgearbeiteten Punkte lässt sich die Zuverlässigkeit der Quantenschlüsselverteilungsplattform steigern.

Abbildungsverzeichnis

Literaturverzeichnis

[1] Ralf Dörner, Stefan Göbel, Wolfgang Effelsberg, Josef Wiemeyer : Serious Games: Foundations, Concepts and Practice. Springer, 2016.

[2] kryptowissen.de; https://www.kryptowissen.de/quantenkryptographie.php, Stand 08.04.2021

[3] kryptowissen.de; https://www.kryptowissen.de/quantenschluesselaustausch.php, Stand 08.04.2021

[4] dtecbw.de; Helmbrecht, Udo : MuQuaNet – Das Quanten-Internet im Großraum München; https://dtecbw.de/home/forschung/unibw-m/projekt-muquanet/projekt-muquanet, Stand 23.04.2021

[5] Bennett, Charles H. und Brassard, Gilles: Quantum cryptography: Public key distribution and coin tossing . In: Theoretical Computer Science 560, Seiten 7-11, 2014. (Abdruck des Originalpapers von 1984)

[6] Universität der Bundeswehr München; Körfgen, Hedwig : Präsentation MuQuaNet, Stand 23.04.2021

[7] Id Quantique; https://www.idquantique.com/quantum-safe-security/products/clavis3-qkd-platform-rd/ : Clavis3 QKD Platform_Brochure, Stand 26.05.2021

[8] Id Quantique; IDQ QKD Cockpit User Guide (v0.6)

[9] Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani and Hugo Zbinden : Fast and simple one-way quantum key distribution. In: APPLIED PHYSICS LETTERS 87, 194108, 2005.

[10] Id Quantique : Quantum Key Distribution System Clavis3 User Guide (v.2.3)

[11] Id Quantique : Christopher Janes; Director, Technical Solutions and Support Worldwide; christopher.janes@idquantique.com

[12] Universität der Bundeswehr München; Lienert, Matthias : Versuchsaufbau DWDM, Stand 29.06.2021

Anhang A

Skript zum Extrahieren der Daten aus den Logfiles

```
1  {
2    import numpy as np
3
4  stdnameq = "DateienIn/Verdunkelte-Messungen-20210423-20210426/AlleQber
       .txt" #Dateipfad
5  stdnamek = "DateienIn/Verdunkelte-Messungen-20210423-20210426/
       AlleSecret.txt" #Dateipfad
6  stdnamev = "DateienIn/Verdunkelte-Messungen-20210423-20210426/
       AlleVisibility.txt" #Dateipfad
7  fname = "DateienIn/Langzeitmessungen2-20210428-20210506/Eve und
       Langzeit2.txt"  # Dateipfad
8  datum = "2021-05-06"  # filter nach Datum
9  QBER = "QBER" #filter nach QBER
10 Visibility = "Visibility" #filter nach Visibility
11 Key = "rate" # filter nach key
12 status = "DEBUG"  # filter nach Statuswort
13 stundemin = 12 #filter alles nach(Zeit) dieser Stunde
14 stundemax = 12 #filter alles vor(Zeit) dieser Stunde
15 minutenmin = 18 #filter alles nach(Zeit) dieser Minute
16 minutenmax = 20 #filter alles vor(Zeit) dieser Minute
17 q = [] #Array QBER
18 v = [] #Array Visibility
19 k = [] #Array KEY
20 stdq =[] #array Standardabweichung f r Eve
21 stdk =[] #array Standardabweichung f r Eve
22 stdv =[] #array Standardabweichung f r Eves
23
24
25 stdqfile= open(stdnameq, "r")
26 stdkfile= open(stdnamek, "r")
27 stdvfile= open(stdnamev, "r")
28 file = open(fname, "r")  # filehandler des fname
29 qfile = open("Testq.txt", "w+")  # filehandler zum schreiben einer
       neuen Datei
```

```
30 qvmfile = open("DateienOut/Langzeitmessung-20210401-20210408/Test -
       QBER.txt","a+") # filehandler zum schreiben einer neuen Datei
31 vfile = open("Testv.txt", "w+")  # filehandler zum schreiben einer
       neuen Datei
32 vvmfile = open("DateienOut/Langzeitmessung-20210401-20210408/Test -
       Visibility.txt","a+") # filehandler zum schreiben einer neuen
       Datei
33 kfile = open("Testk.txt", "w+")  # filehandler zum schreiben einer
       neuen Datei
34 kvmfile = open("DateienOut/Langzeitmessung-20210401-20210408/Test -
       Actual key rate.txt","a+") # filehandler zum schreiben einer neuen
        Datei
35 filek = open("DateienOut/Verdunkelte-Messungen-20210423-20210426/
       Actual key rate.txt","a+")
36 filev = open("DateienOut/Verdunkelte-Messungen-20210423-20210426/
       Visibility.txt","a+")
37 fileq = open("DateienOut/Verdunkelte-Messungen-20210423-20210426/QBER.
       txt","a+")
38
39 # for line in stdqfile:
40 #     value = line.split()[0]
41 #     stdq.append(float(value))
42 #
43 # a = f"{np.mean(stdq)}  {np.std(stdq)}\n"
44 #
45 # fileq.write(a)
46 #
47 # for line in stdkfile:
48 #     value = line.split()[0]
49 #     stdk.append(float(value))
50 #
51 # b = f"{np.mean(stdk)}  {np.std(stdk)}\n"
52 #
53 # filek.write(b)
54 #
55 # for line in stdvfile:
56 #     value = line.split()[0]
57 #     stdv.append(float(value))
58 #
59 # c = f"{np.mean(stdv)} {np.std(stdv)}\n"
60 #
61 # filev.write(c)
62 #
63
64
65 for line in file:
66     if QBER in line:
67         if datum in line:
68             if status in line:
69                 date = line.split()[0][0:10]  # rausschreiben Datum
70                 time = line.split()[0][11:]#.replace(":",".")  #
                       rausschreiben Uhrzeit ( replace Doppelpunkt durch
                       Punkt, wenn gnuplot keine Doppelpunkte akzeptiert
```

```
71                  hour = int(line.split()[0][11:].split(":")[0])  #
                        rausschreiben Stunde als Int zum filtern
72                  minutes = int(line.split()[0][11:].split(":")[1])  #
                        rausschreiben Minute als Int zum filtern
73                  if stundemin <= hour <= stundemax and minutenmin <=
                        minutes <= minutenmax:  # filter alles zwischen
                        dieser Uhrzeit
74                      time1 = time #letzte Zeit in meinem angegebenen
                            Intervall
75                      value = line.split()[-1]  # schreibe Letzten Wert
                            raus ( QBER, Visibility)
76
77                      try:
78                          float(value)  # ist value eine float
79
80                      except ValueError:
81                          continue  # wenn nicht,    berspringe    diese
                                Zeile
82                      # array = line.split()
83                      q.append(float(value)) #Werte dem Array
                            hinzuf gen
84
85                      s = f" {value}\n"  # Format was in die Datei kommt
86
87                      qfile.write(s)  # schreibe Werte in Datei
88
89 m = f"{time1}    {np.mean(q)}    {np.std(q)}\n" #schreibe Mittelwert
       und Standardabweichung in Array (QBER, Visibility)
90
91 qvmfile.write(m)
92
93 file.close()
94 file = open(fname, "r")  # filehandler des fname
95 for line in file:
96     if Visibility in line:
97         if datum in line:
98             if status in line:
99                 date = line.split()[0][0:10]  # rausschreiben Datum
100                time = line.split()[0][11:]#.replace(":",".")  #
                        rausschreiben Uhrzeit ( replace Doppelpunkt durch
                        Punkt, wenn gnuplot keine Doppelpunkte akzeptiert
101                hour = int(line.split()[0][11:].split(":")[0])  #
                        rausschreiben Stunde als Int zum filtern
102                minutes = int(line.split()[0][11:].split(":")[1])  #
                        rausschreiben Minute als Int zum filtern
103                if stundemin <= hour <= stundemax and minutenmin <=
                        minutes <= minutenmax:  # filter alles zwischen
                        dieser Uhrzeit
104                    time1 = time #letzte Zeit in meinem angegebenen
                            Intervall
105                    value = line.split()[-1]  # schreibe Letzten Wert
                            raus ( QBER, Visibility)
106
```

```
107                     try:
108                         float(value)  # ist value eine float
109
110                     except ValueError:
111                         continue  # wenn nicht,  berspringe  diese
                                Zeile
112                     # array = line.split()
113                     if 0 <= float(value) <= 1.1:
114                         v.append(float(value)) #Werte dem Array
                                hinzuf gen
115
116                     t = f" {value}\n"  # Format was in die Datei kommt
117
118                     vfile.write(t)  # schreibe Werte in Datei
119
120 n = f"{time1}    {np.mean(v)}   {np.std(v)}\n" #schreibe Mittelwert
    und Standardabweichung in Array (QBER, Visibility)
121
122 vvmfile.write(n)
123
124 file.close()
125 file = open(fname, "r")  # filehandler des fname
126 for line in file:
127     if Key in line:
128         if datum in line:
129             if status in line:
130                 date = line.split()[0][0:10]  # rausschreiben Datum
131                 time = line.split()[0][11:]#.replace(":",".")  #
                        rausschreiben Uhrzeit ( replace Doppelpunkt durch
                        Punkt, wenn gnuplot keine Doppelpunkte akzeptiert
132                 hour = int(line.split()[0][11:].split(":")[0])  #
                        rausschreiben Stunde als Int zum filtern
133                 minutes = int(line.split()[0][11:].split(":")[1])  #
                        rausschreiben Minute als Int zum filtern
134                 if stundemin <= hour <= stundemax and minutenmin <=
                        minutes <= minutenmax:  # filter alles zwischen
                        dieser Uhrzeit
135                     time1 = time #letzte Zeit in meinem angegebenen
                            Intervall
136                     value = line.split()[-2]  # schreibe Letzten Wert
                            raus ( Key)
137
138                     try:
139                         float(value)  # ist value eine float
140
141                     except ValueError:
142                         continue  # wenn nicht,  berspringe  diese
                                Zeile
143                     # array = line.split()
144                     if float(value) <= 3000:
145                         k.append(float(value)) #Werte dem Array
                                hinzuf gen
146
```

```
147                         u = f"  {value}\n"  # Format was in die Datei
                                kommt
148
149                         kfile.write(u)  # schreibe Werte in Datei
150
151 o = f"{time1}     {np.mean(k)}    {np.std(k)}\n" #schreibe Mittelwert
        und Standardabweichung in Array (QBER, Visibility)
152
153 kvmfile.write(o)
154
155
156 }
```

Listing A.1: Skript zum Extrahieren der Daten aus den Logfiles

Anhang B

Stabilitätsstudie

B.0.1 Erste Stabilitätsstudie

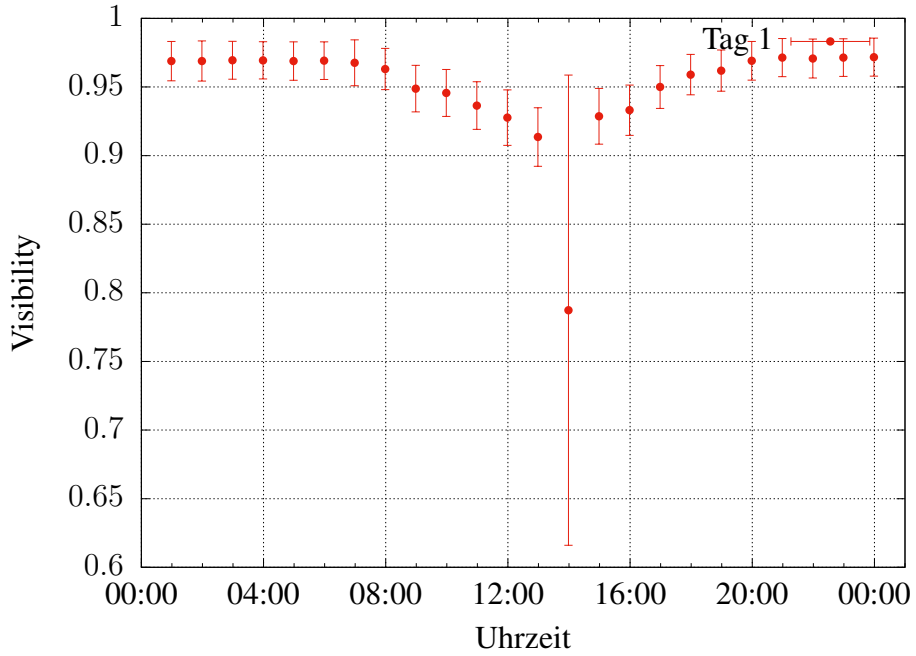

Abbildung B.1: Tag 1 - Visibility - Erweiterter y-Achsenbereich

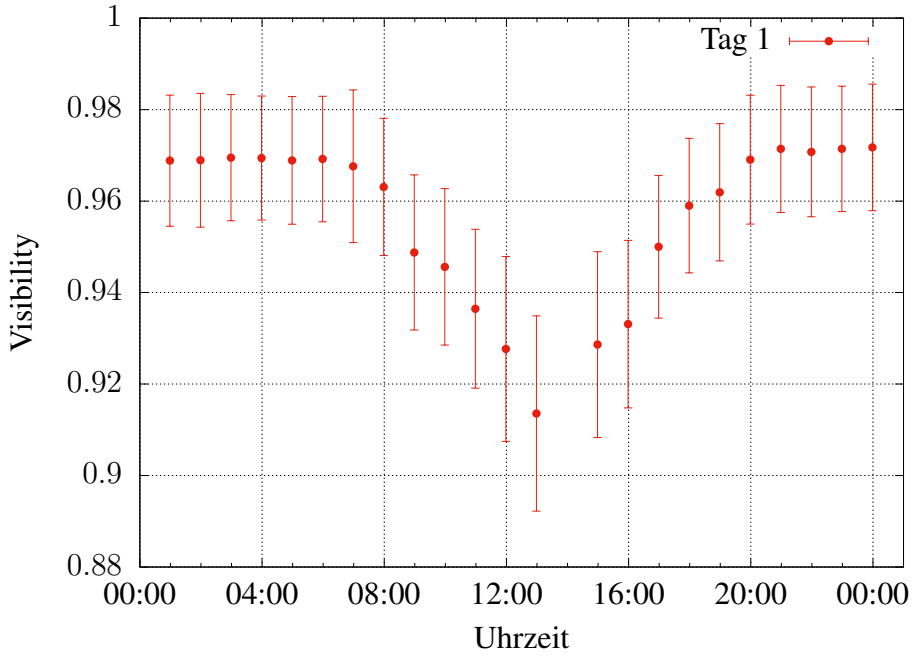

Abbildung B.2: Tag 1 - Visibility

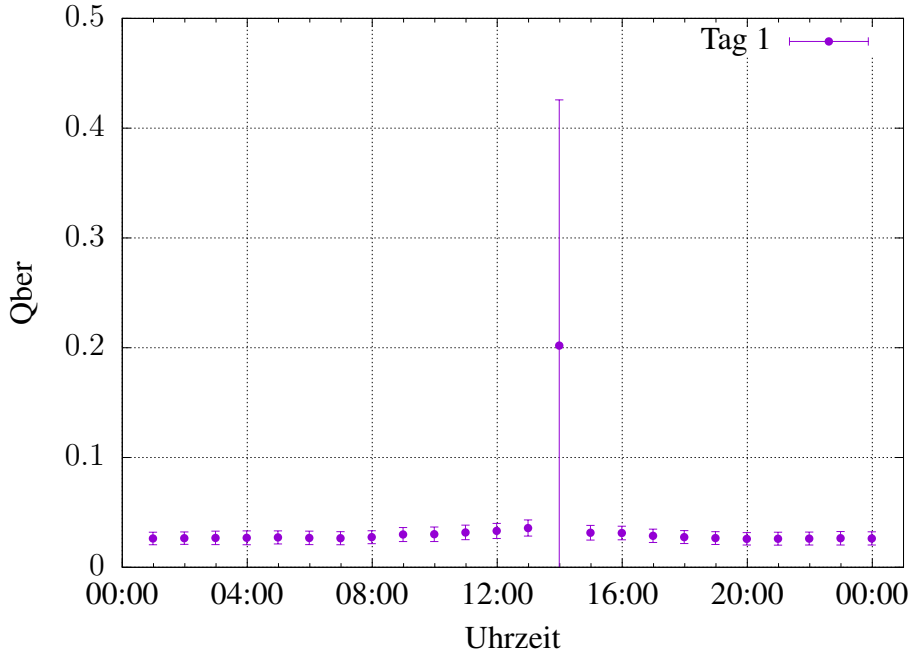

Abbildung B.3: Tag 1 - Qber - Erweiterter y-Achsenbereich

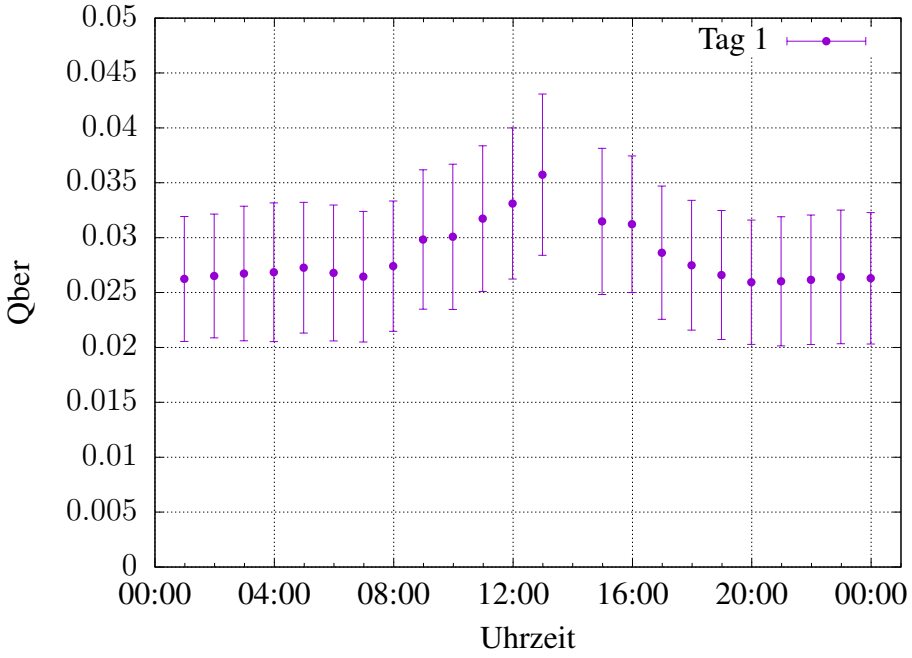

Abbildung B.4: Tag 2 - Qber

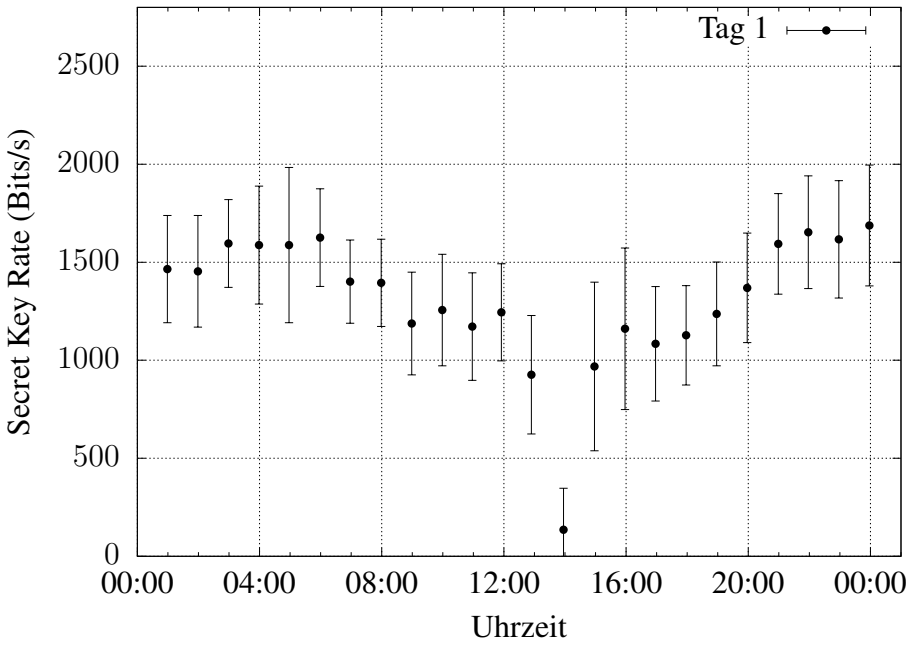

Abbildung B.5: Tag 1 - Secret Key Rate

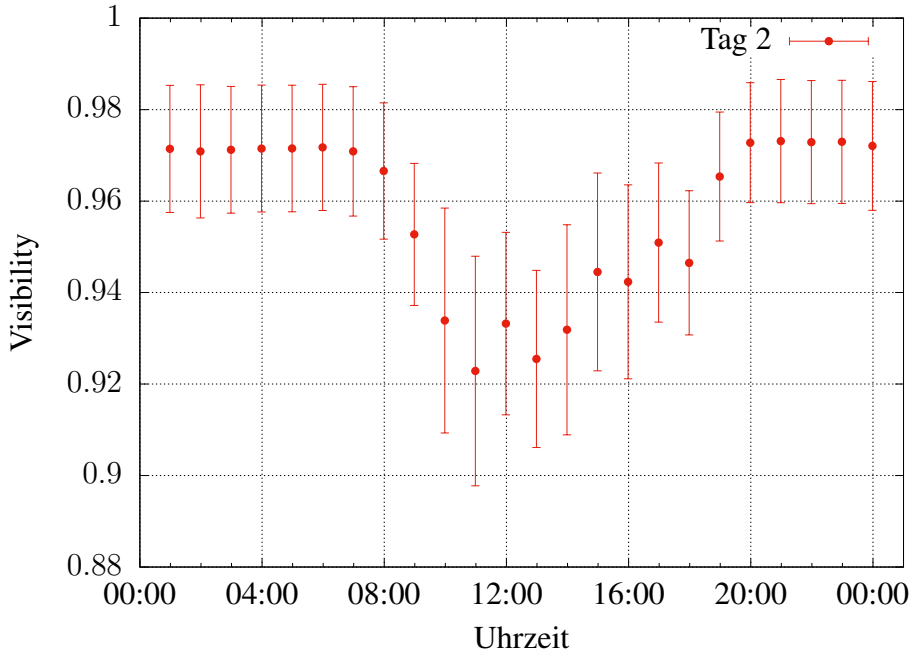

Abbildung B.6: Tag 2 - Visibility

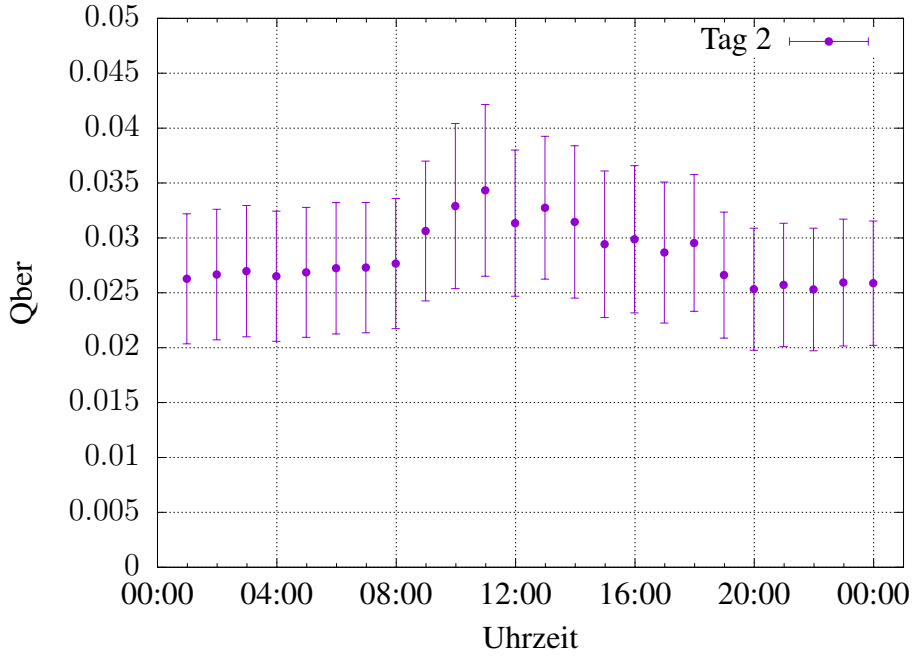

Abbildung B.7: Tag 2 - Qber

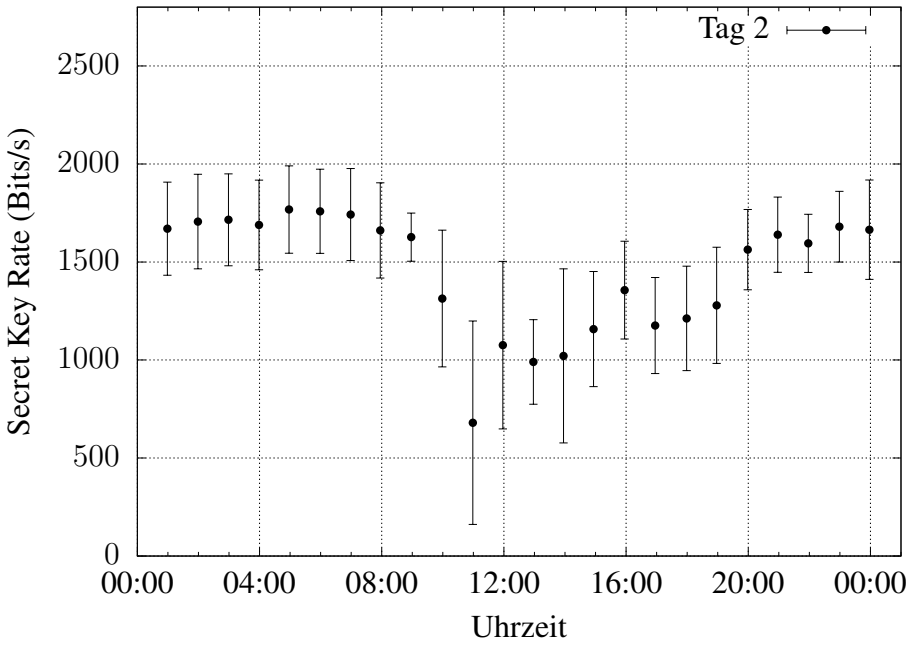

Abbildung B.8: Tag 2 - Secret Key Rate

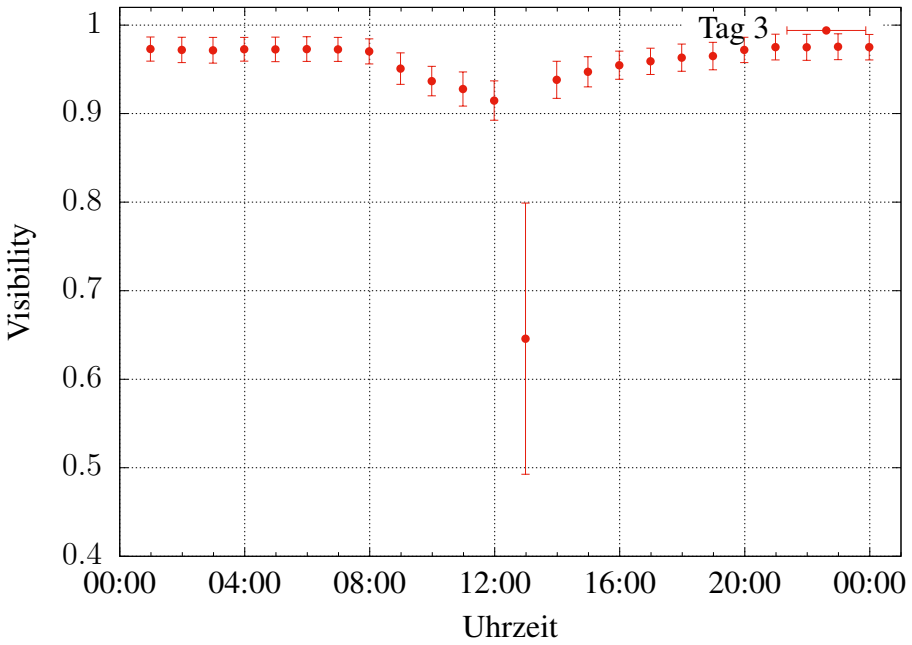

Abbildung B.9: Tag 3 - Visibility - Erweiterter y-Achsenbereich

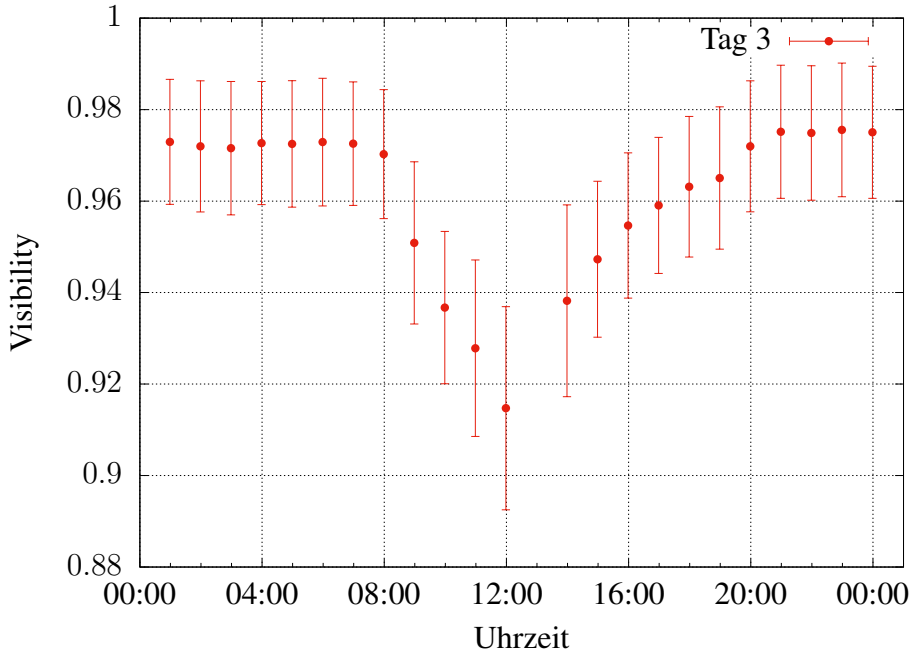

Abbildung B.10: Tag 3 - Visibility

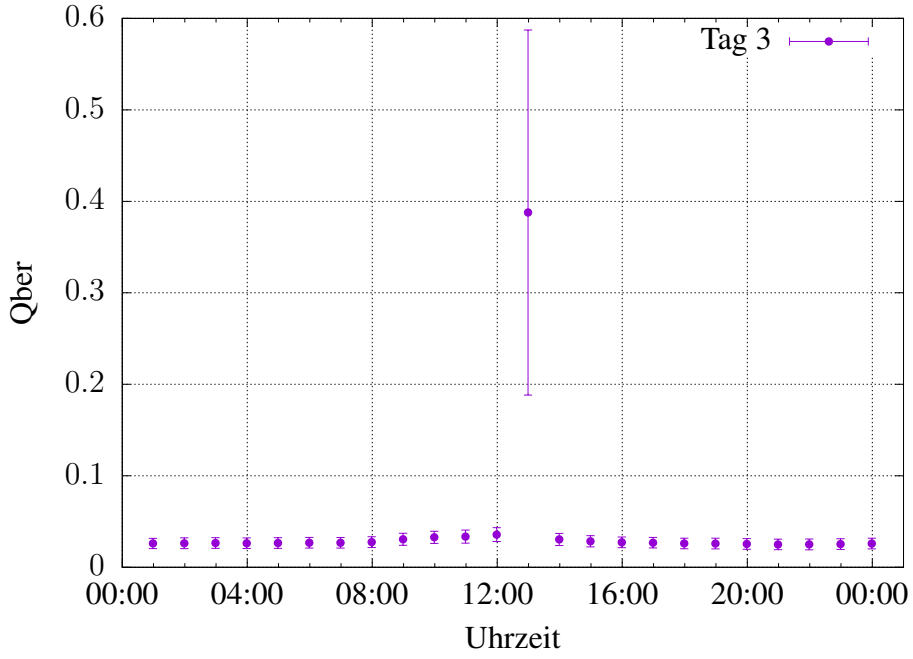

Abbildung B.11: Tag 3 - Qber - Erweiterter y-Achsenbereich

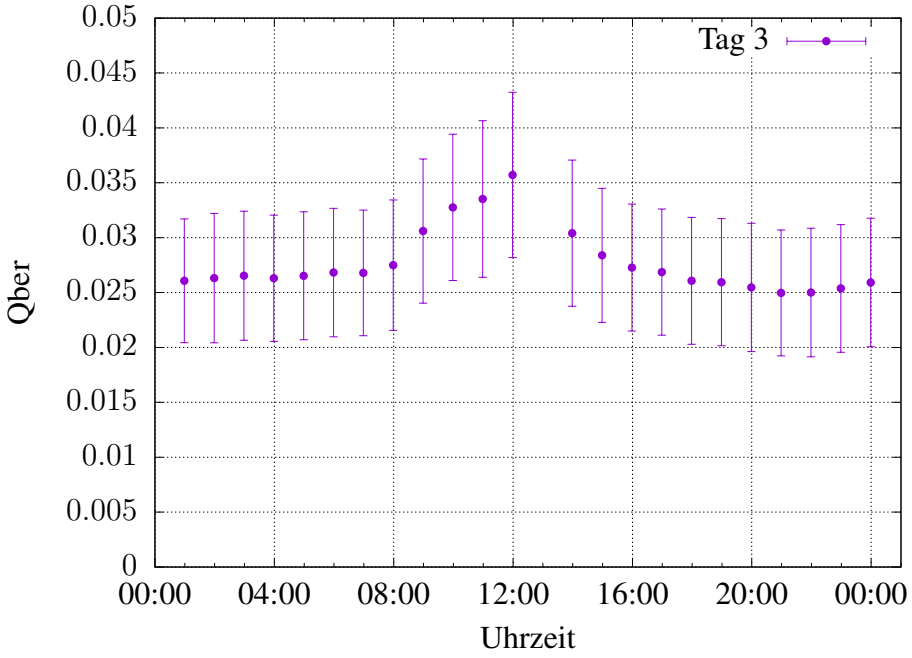

Abbildung B.12: Tag 3 - Qber

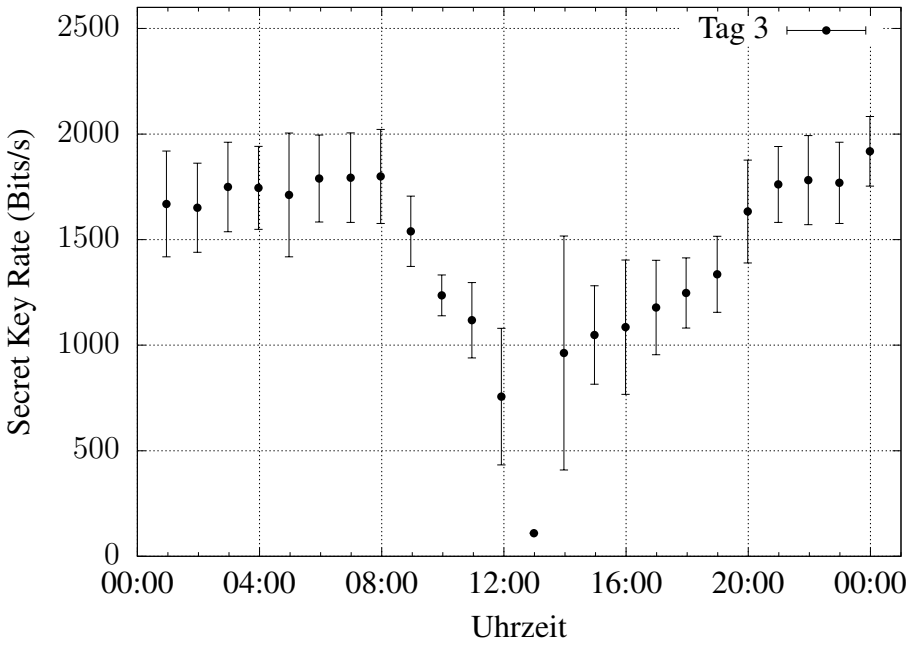

Abbildung B.13: Tag 3 - Secret Key Rate

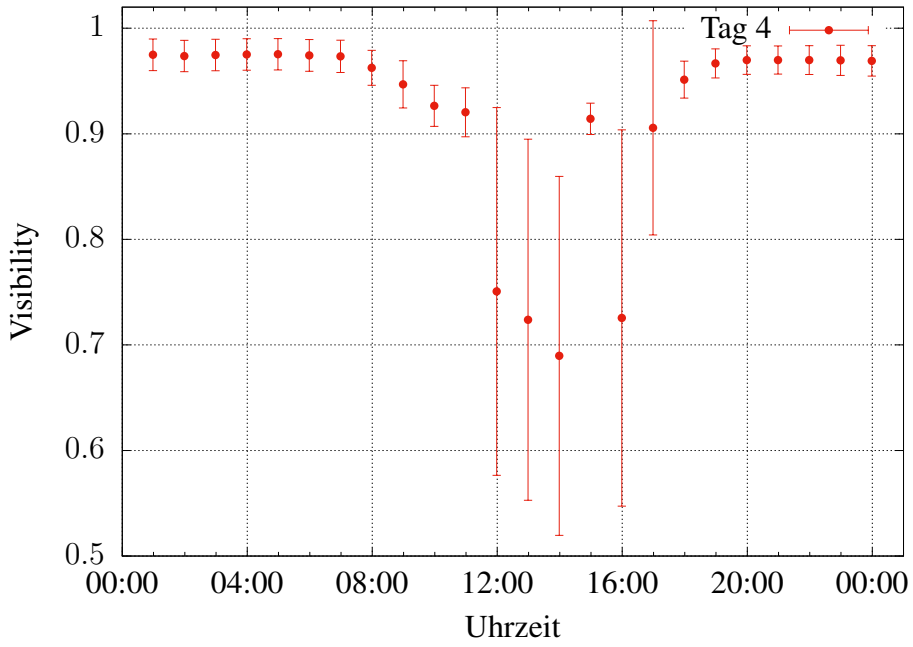

Abbildung B.14: Tag 4 - Visibility - Erweiterter y-Achsenbereich

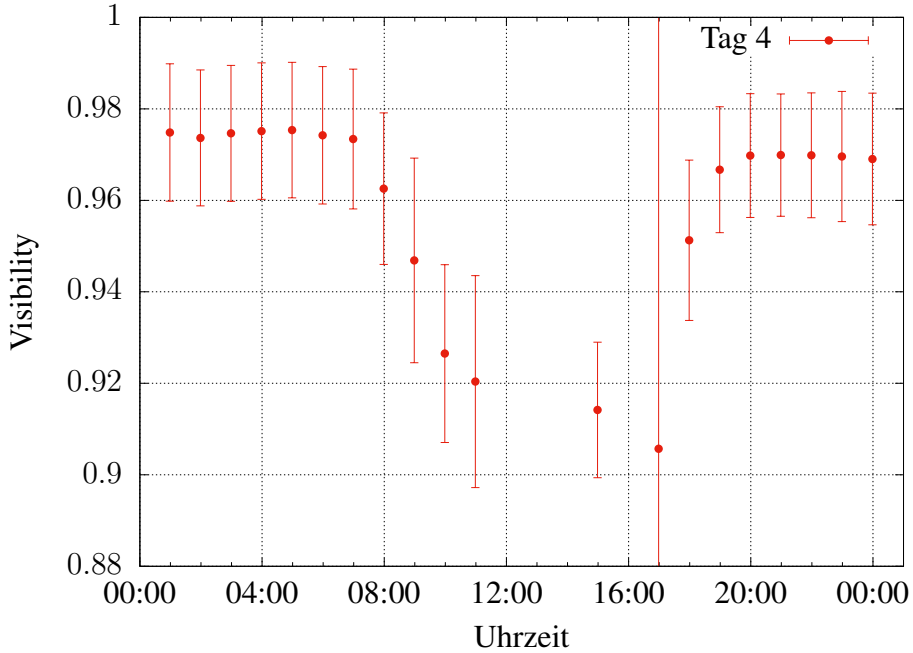

Abbildung B.15: Tag 4 - Visibility

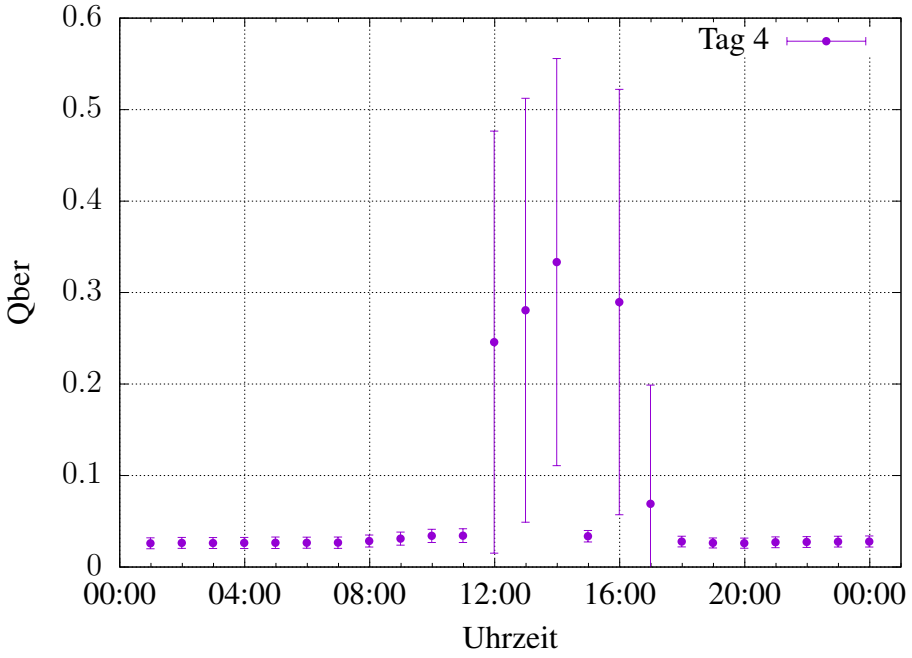

Abbildung B.16: Tag 4 - Qber - Erweiterter y-Achsenbereich

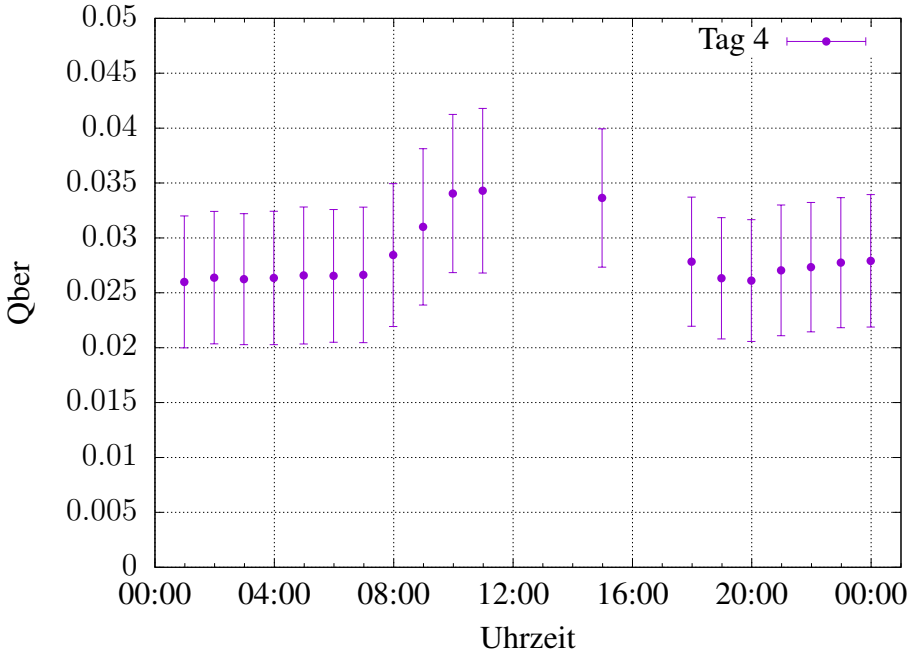

Abbildung B.17: Tag 4 - Qber

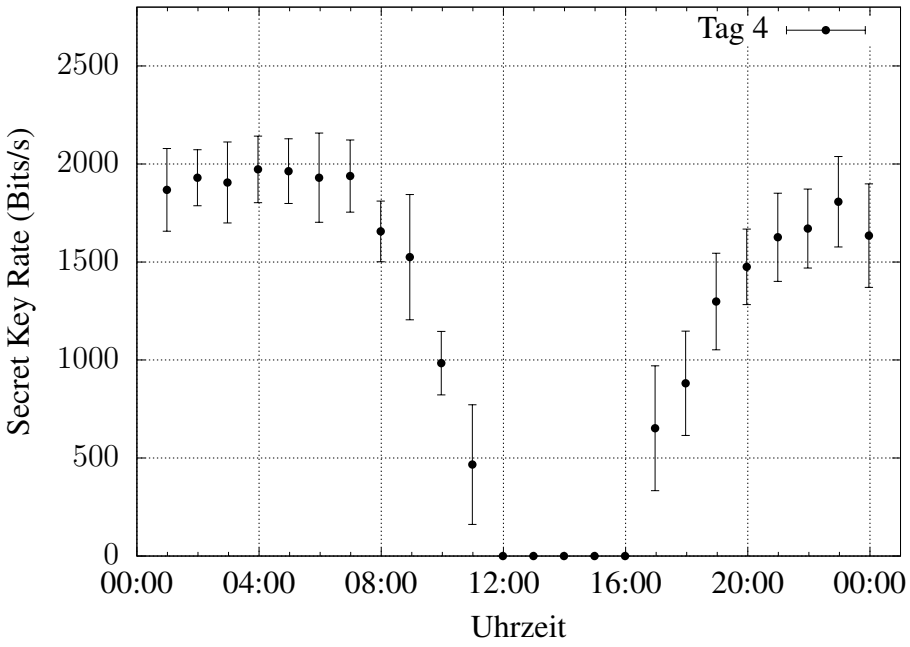

Abbildung B.18: Tag 4 - Secret Key Rate

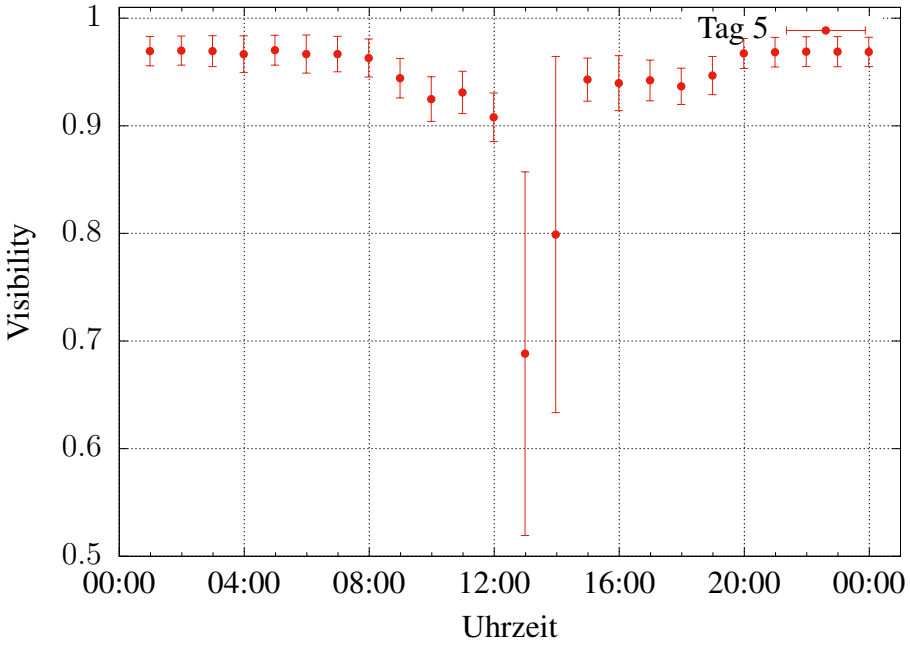

Abbildung B.19: Tag 5 - Visibilty - Erweiterter y-Achsenbereich

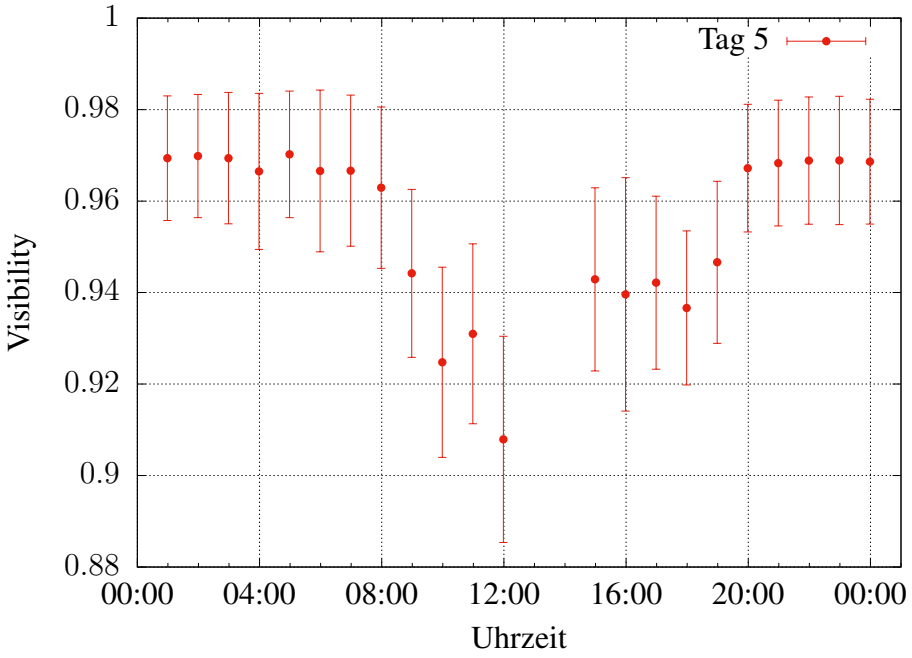

Abbildung B.20: Tag 2 - Visibility

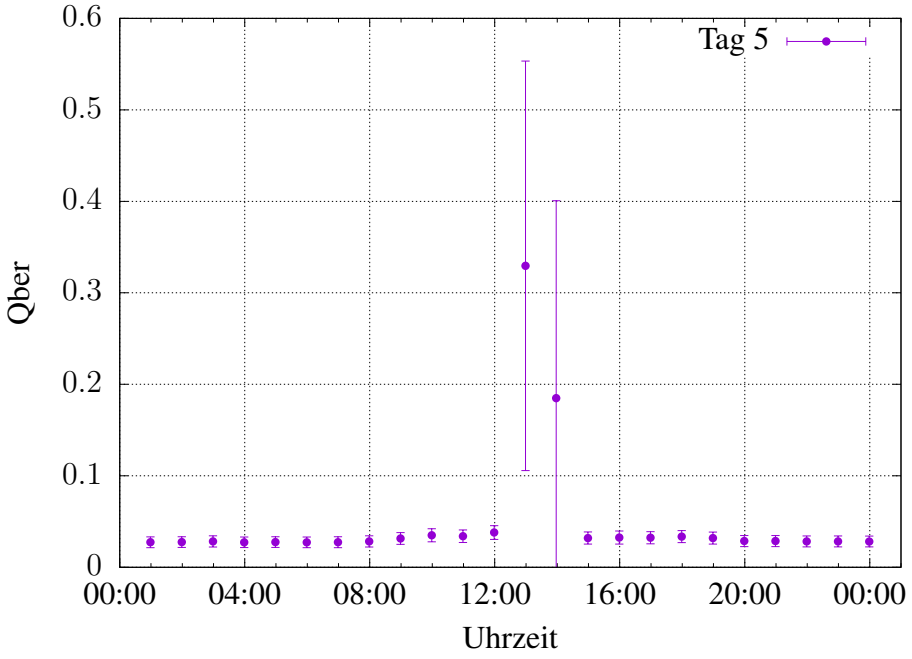

Abbildung B.21: Tag 5 - Qber - Erweiterter y-Achsenbereich

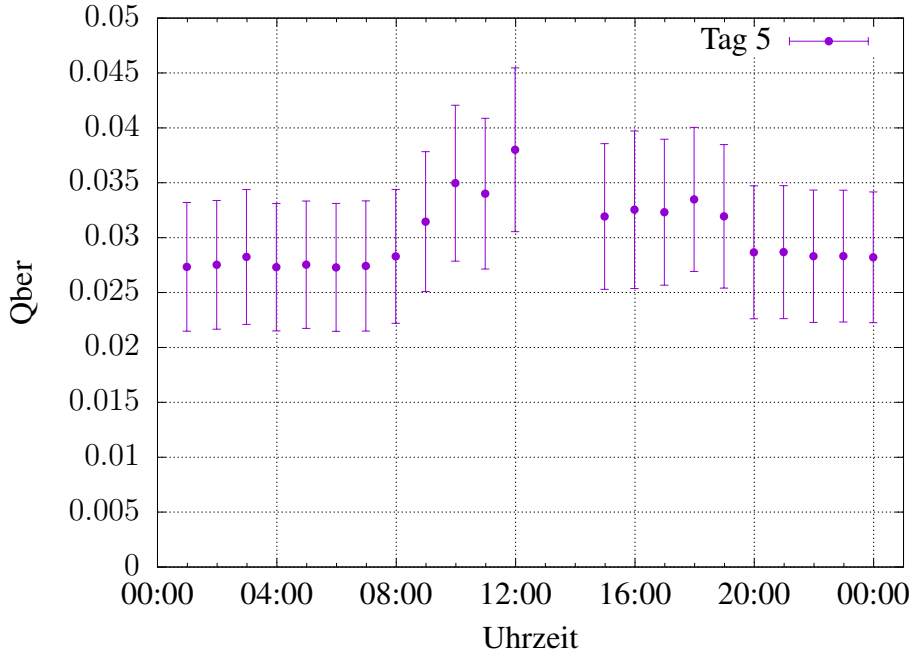

Abbildung B.22: Tag 5 - Qber

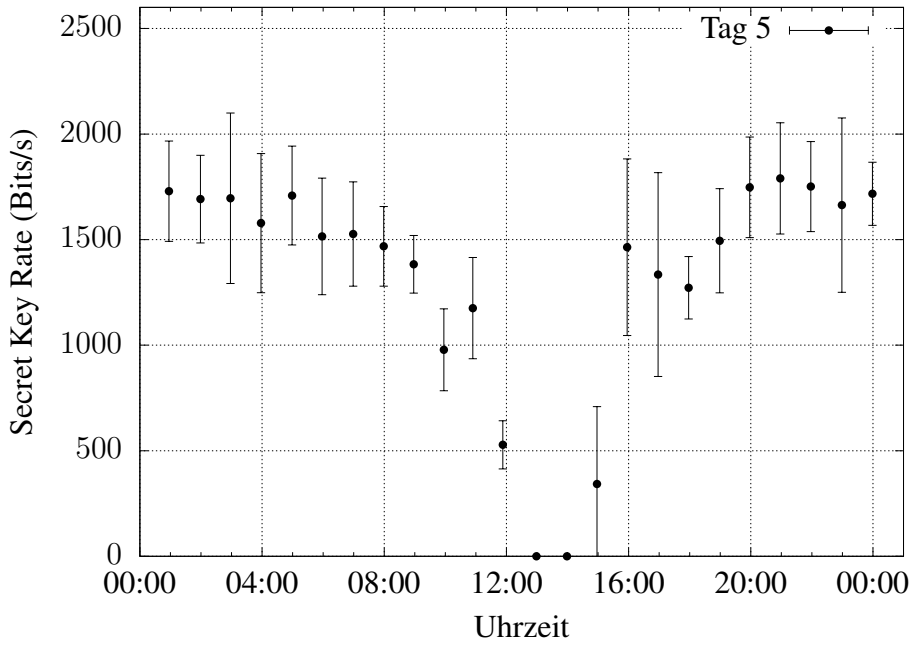

Abbildung B.23: Tag 5 - Secret Key Rate

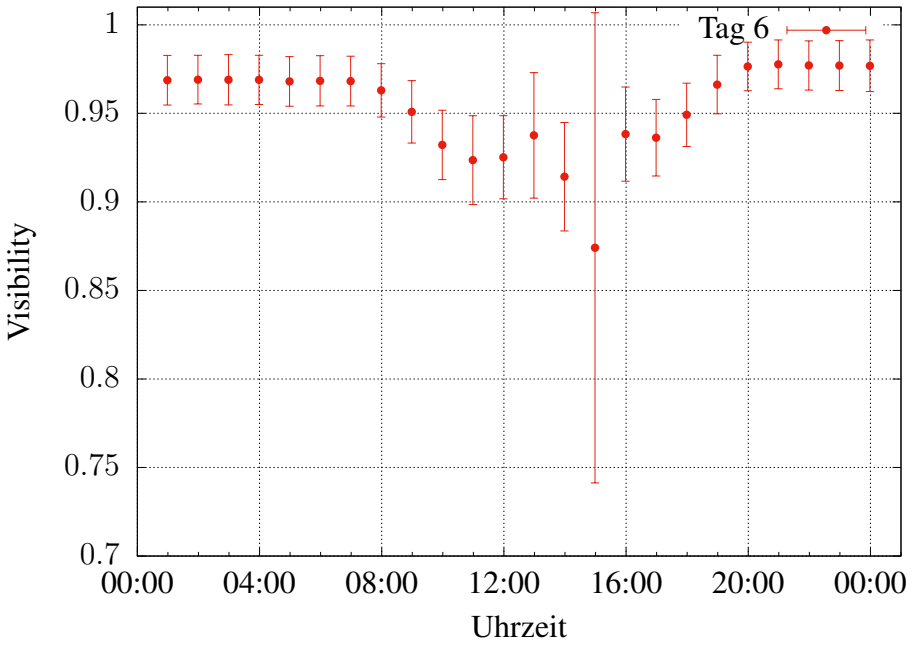

Abbildung B.24: Tag 6 - Visibility - Erweiterter y-Achsenbereich

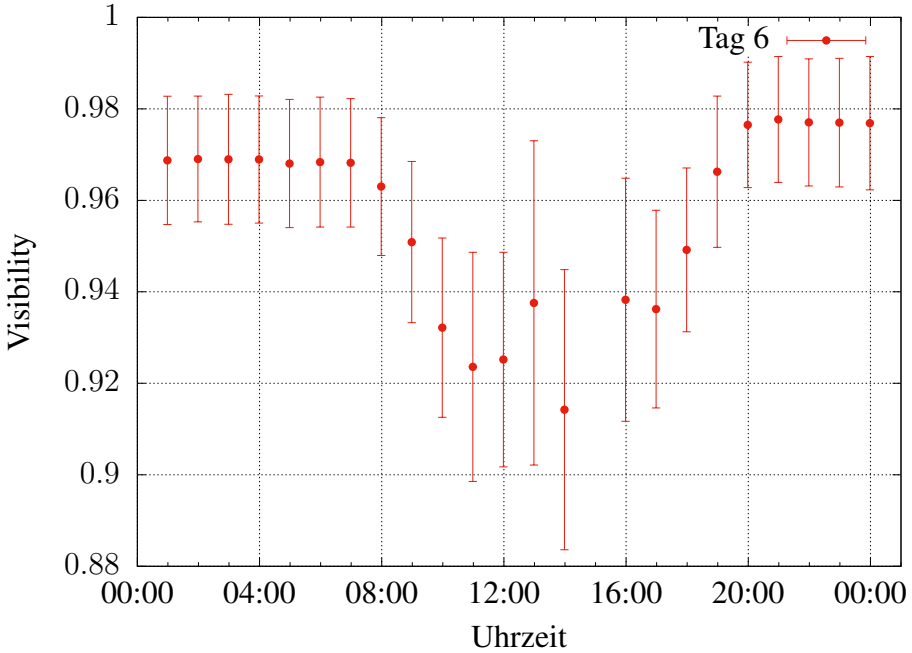

Abbildung B.25: Tag 6 - Visibility

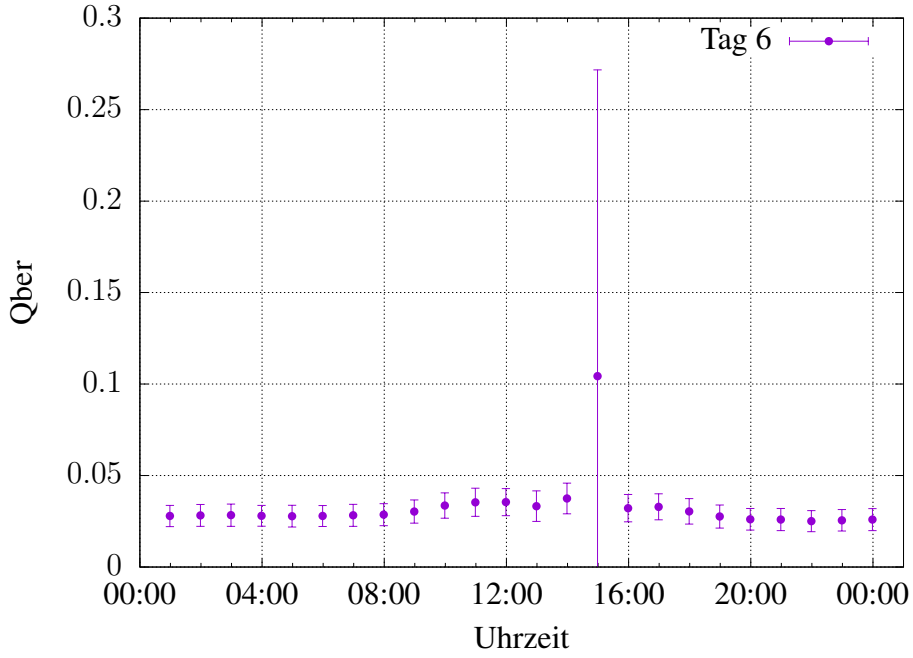

Abbildung B.26: Tag 6 - Qber - Erweiterter y-Achsenbereich

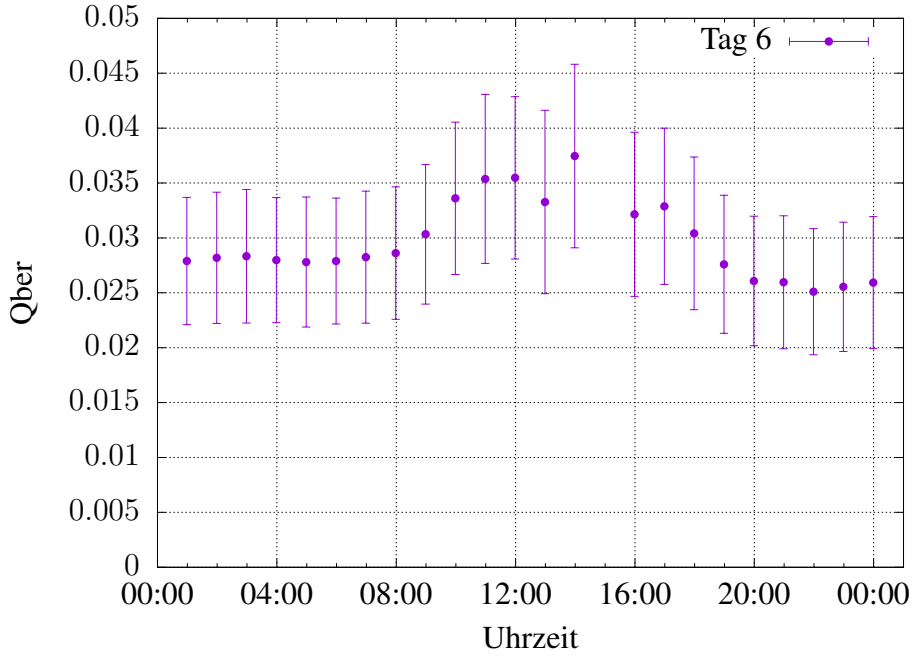

Abbildung B.27: Tag 6 - Qber

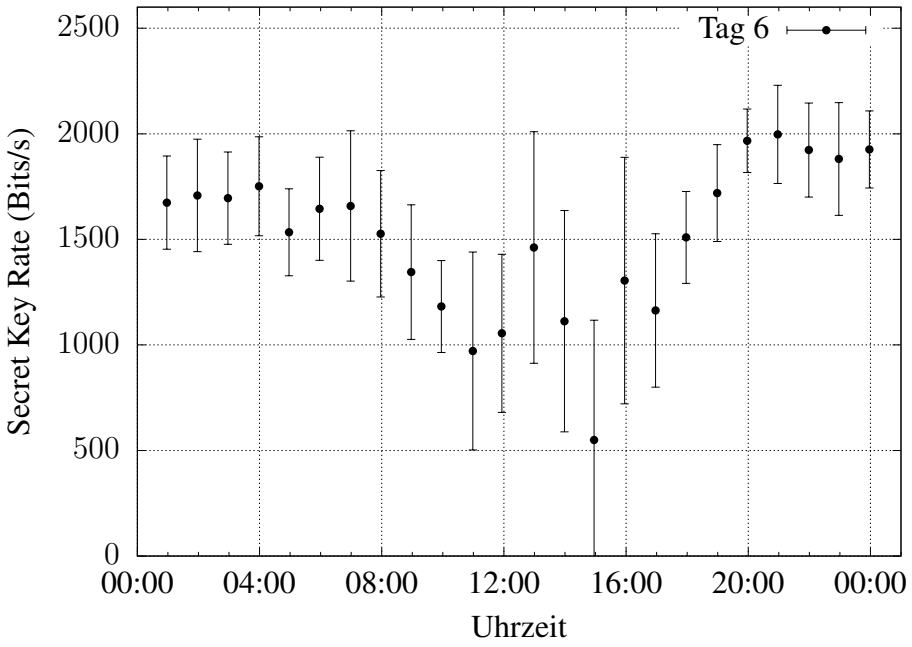

Abbildung B.28: Tag 6 - Secret Key Rate

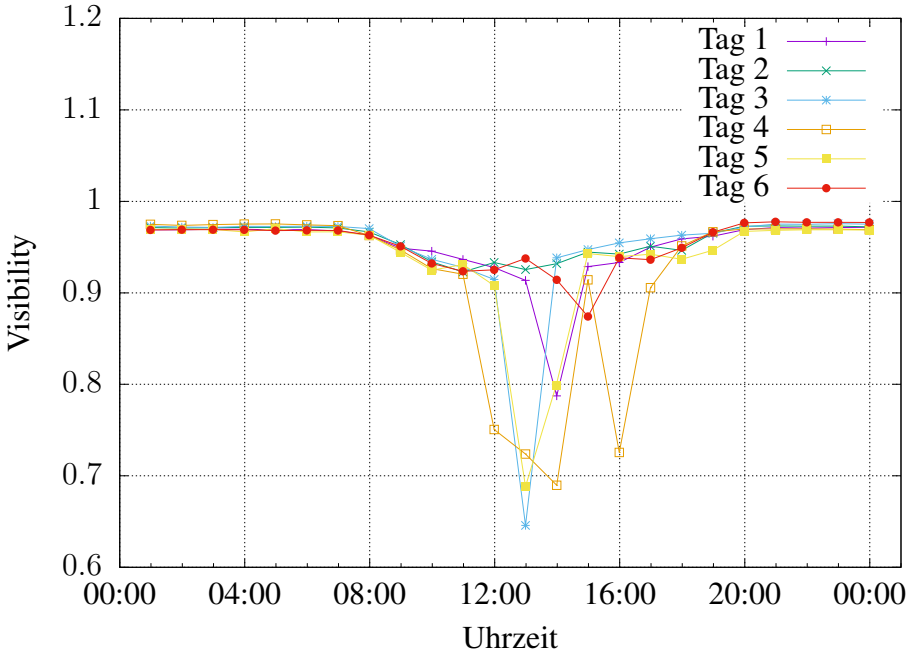

Abbildung B.29: Tag 1-6 - Visibility

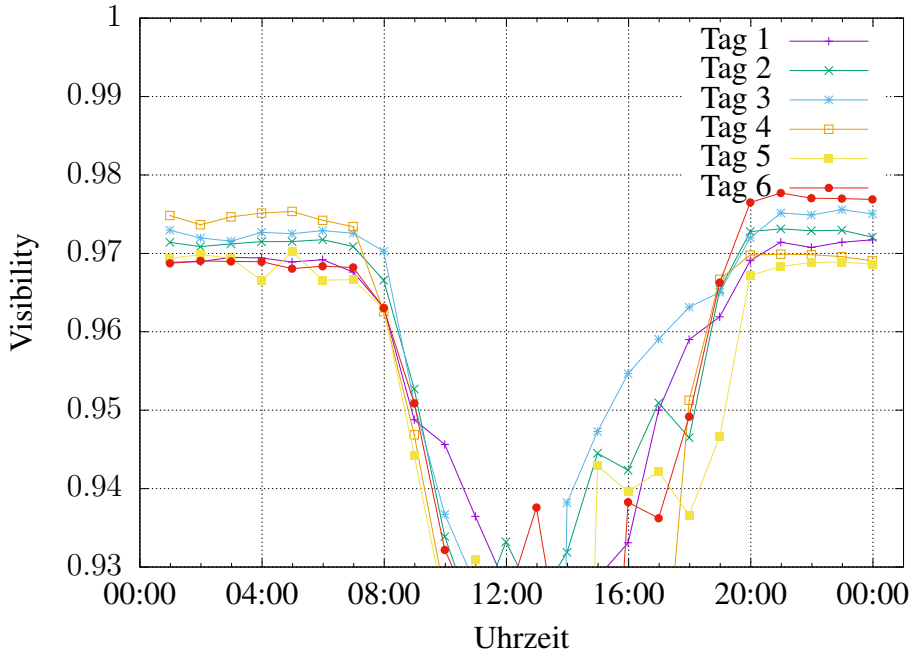

Abbildung B.30: Tag 1-6 - Visibility - Vergrößert

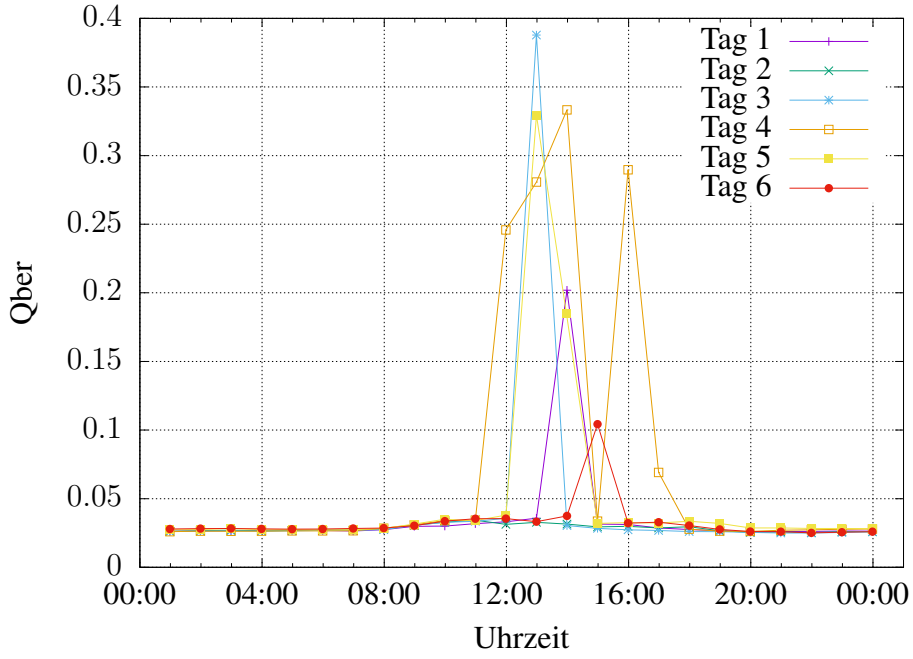

Abbildung B.31: Tag 1-6 - Qber

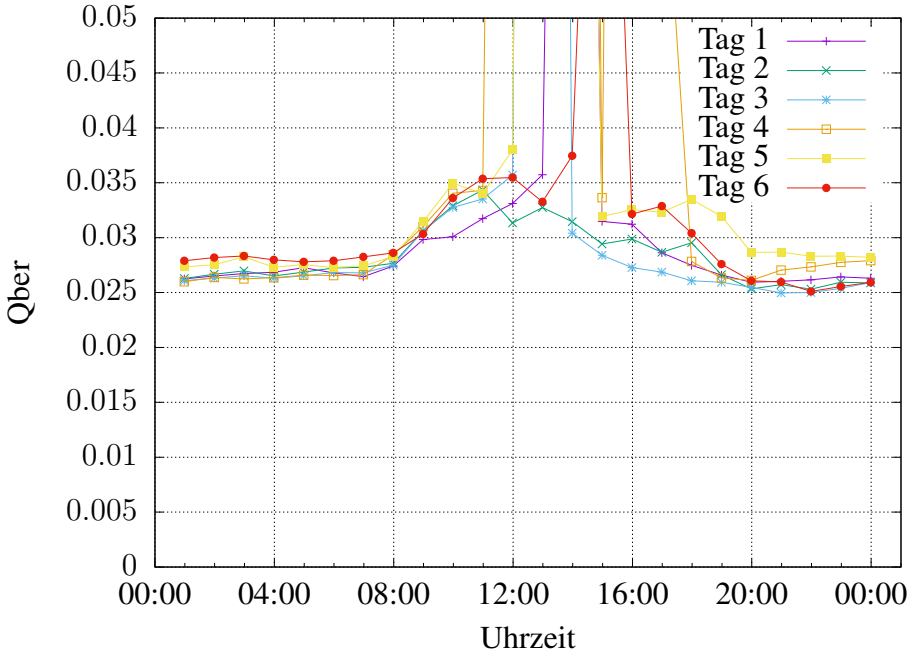

Abbildung B.32: Tag 1-6 - Qber - Vergrößert

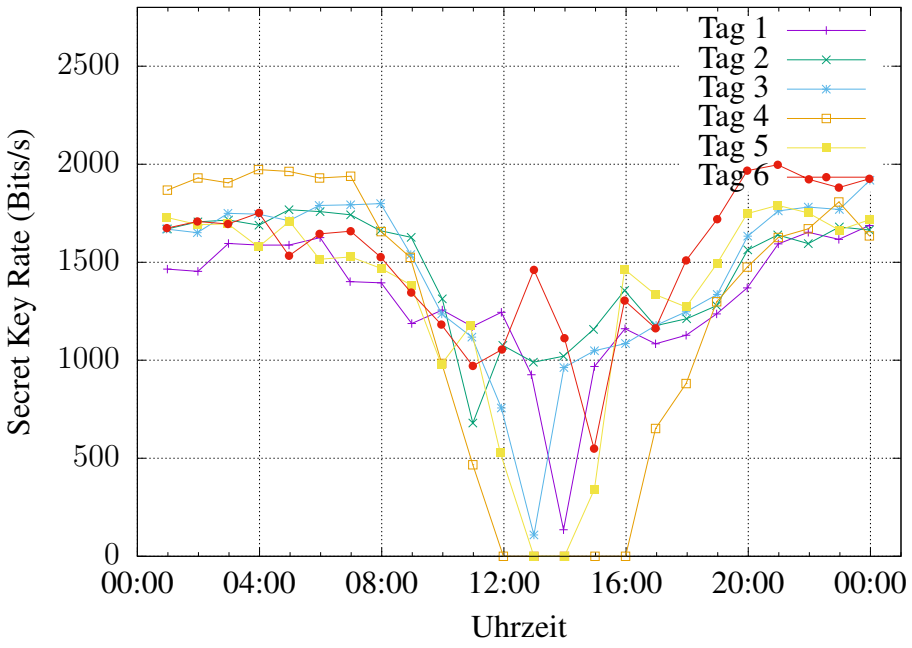

Abbildung B.33: Tag 1-6 - Secret Key Rate

Tabelle B.1: Beobachtete Wetterverhältnisse bei der ersten Stabilitätsmessung

	00:00 - 03:00	03:00 - 06:00	06:00 - 09:00	09:00 - 12:00
Tag 1	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 2	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 3	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 4	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 5	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 6	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt

	12:00 - 15:00	15:00 - 18:00	18:00 - 21:00	21:00 - 24:00
Tag 1	Sonnig	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang
Tag 2	Sonnig, bewölkt	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang
Tag 3	Sonnig	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang
Tag 4	Sonnig	Sonnig	Sonnig, bewölkt	Sonnenuntergang
Tag 5	Sonnig	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang
Tag 6	Sonnig, bewölkt	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang

B.0.2 Zweite Stabilitätsstudie

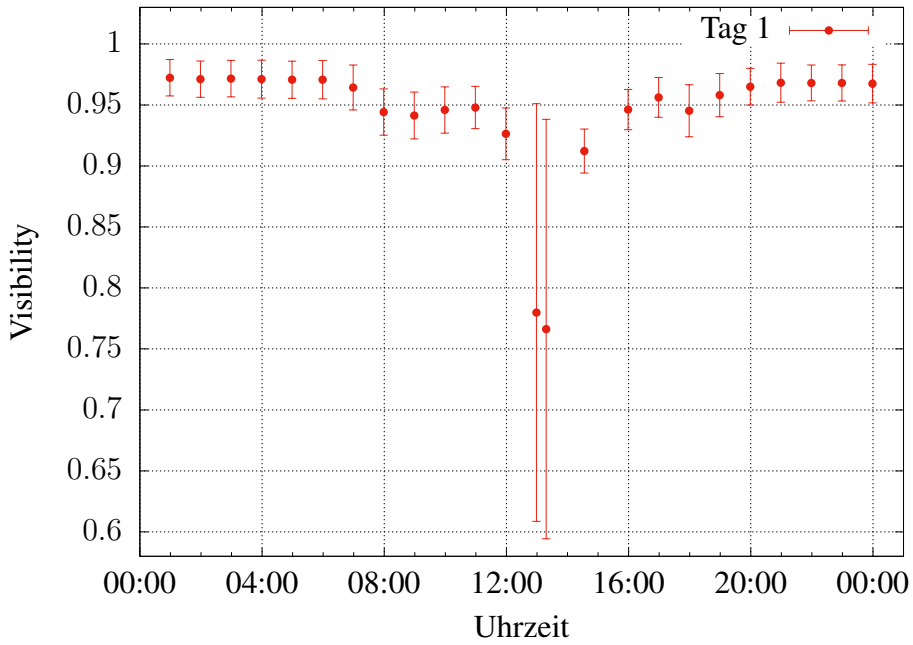

Abbildung B.34: Tag 1 - Visibility - Messung 2 - Erweiterter y-Achsenbereich

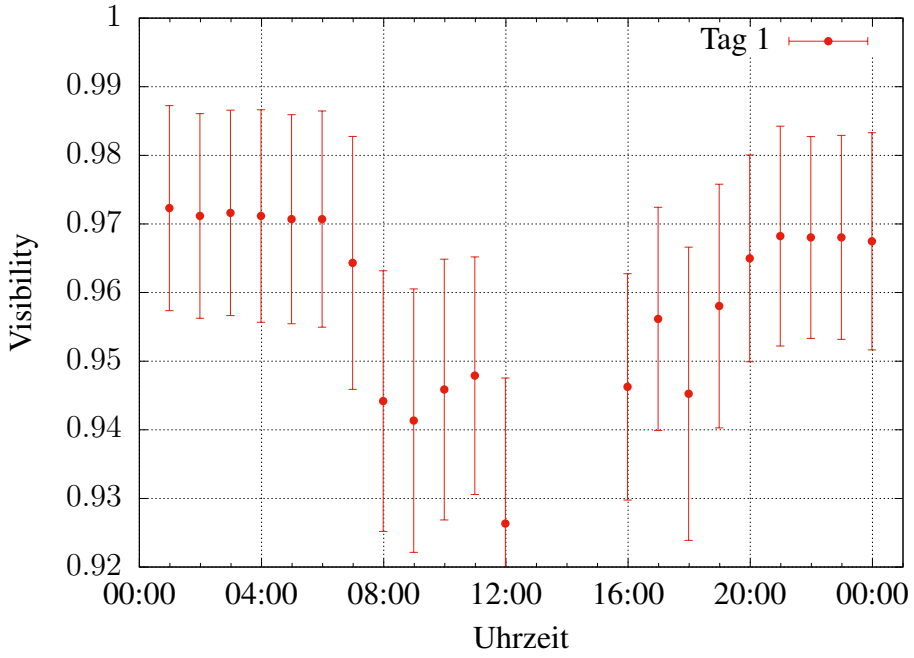

Abbildung B.35: Tag 1 - Visibility - Messung 2

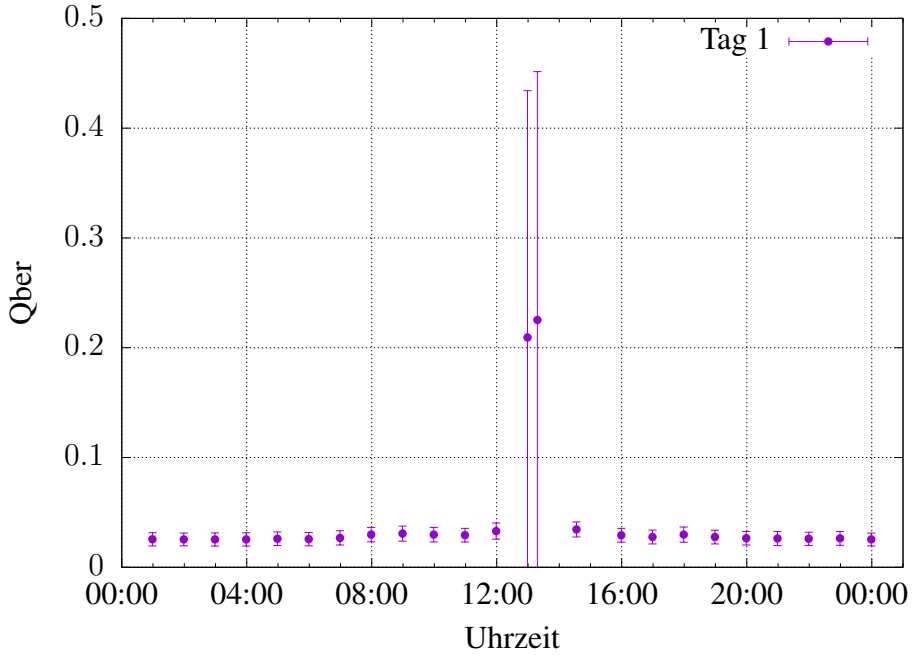

Abbildung B.36: Tag 1 - Qber - Messung 2 - Erweiterter y-Achsenbereich

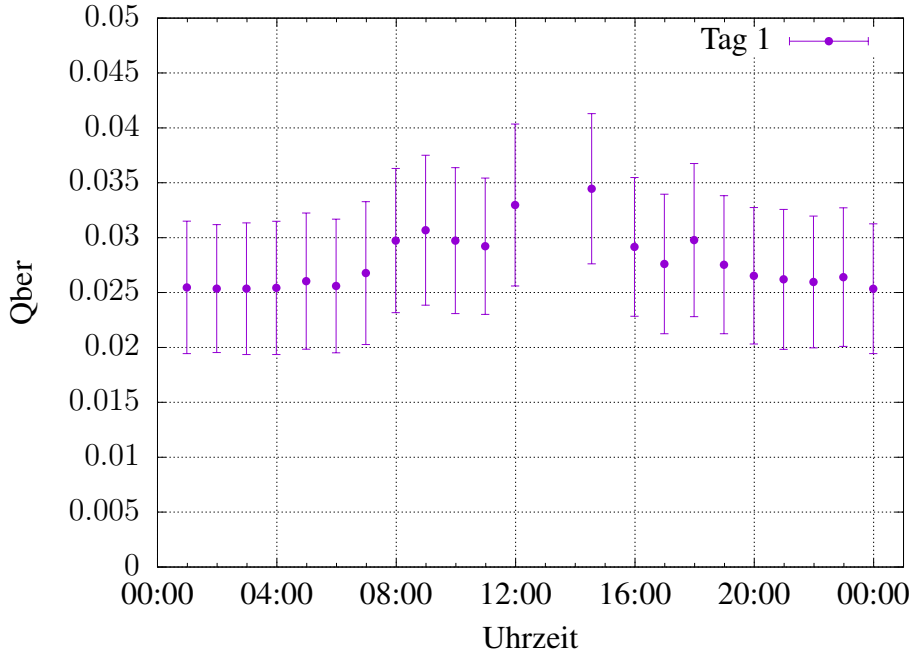

Abbildung B.37: Tag 1 - Qber - Messung 2

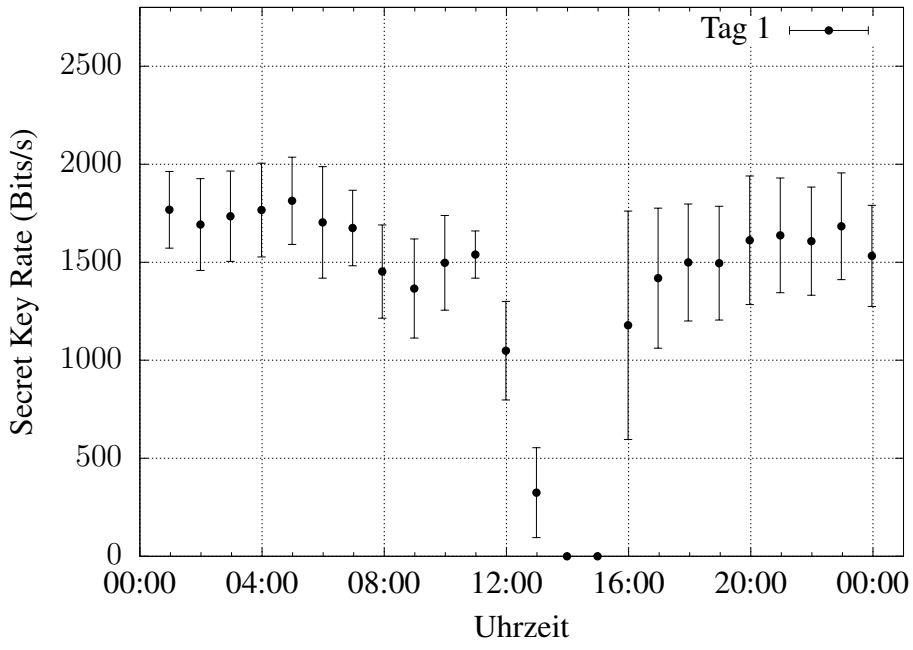

Abbildung B.38: Tag 1 - Secret Key Rate - Messung 2

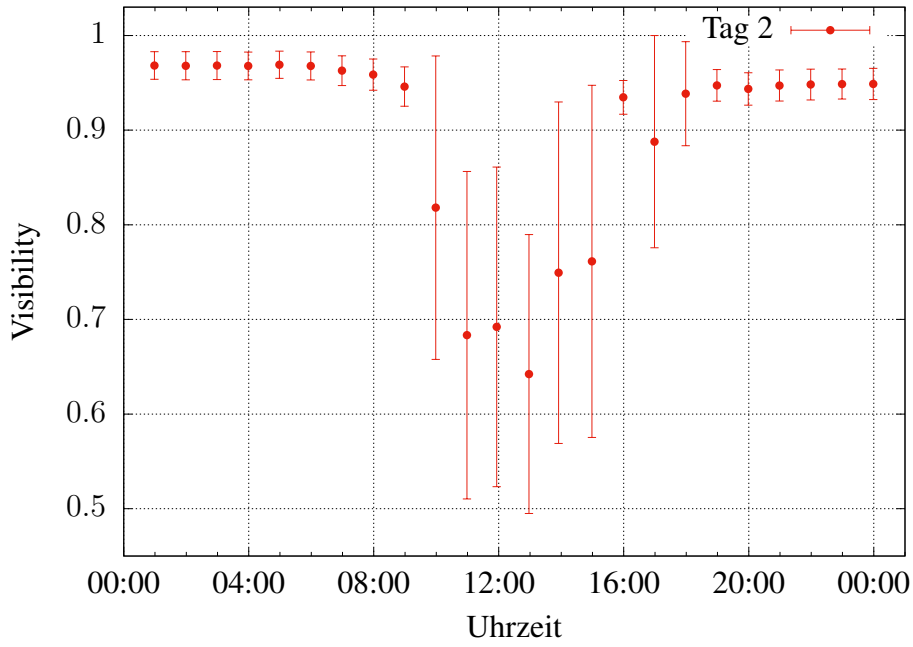

Abbildung B.39: Tag 2 - Visibility - Messung 2 - Erweiterter y-Achsenbereich

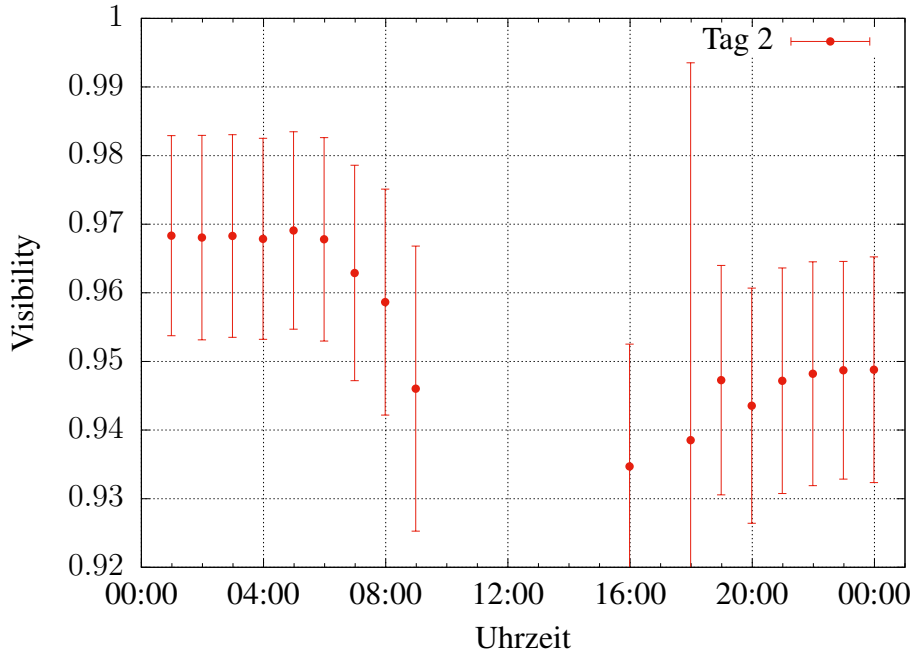

Abbildung B.40: Tag 2 - Visibility - Messung 2

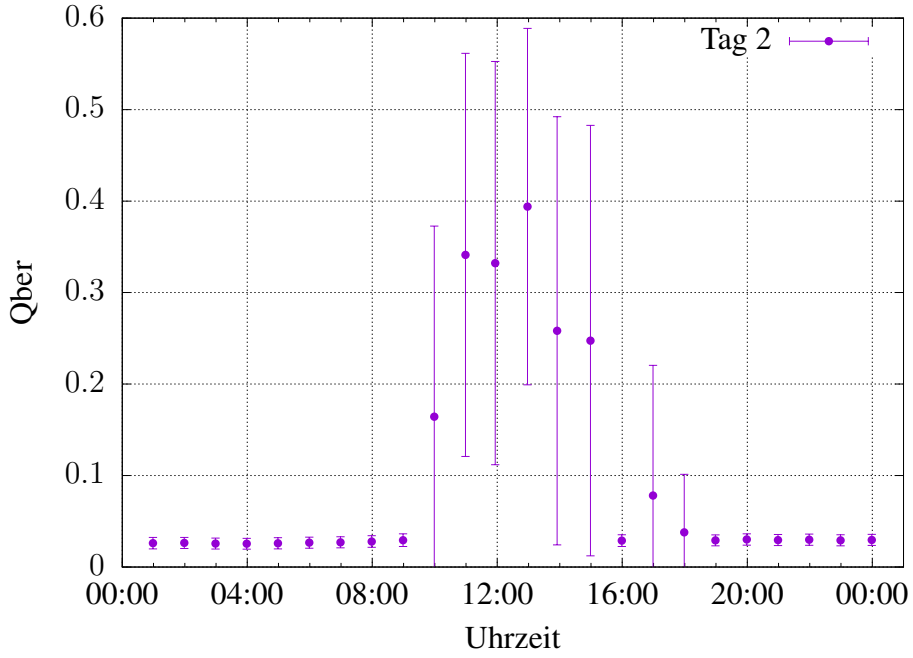

Abbildung B.41: Tag 2 - Qber - Messung 2 - Erweiterter y-Achsenbereich

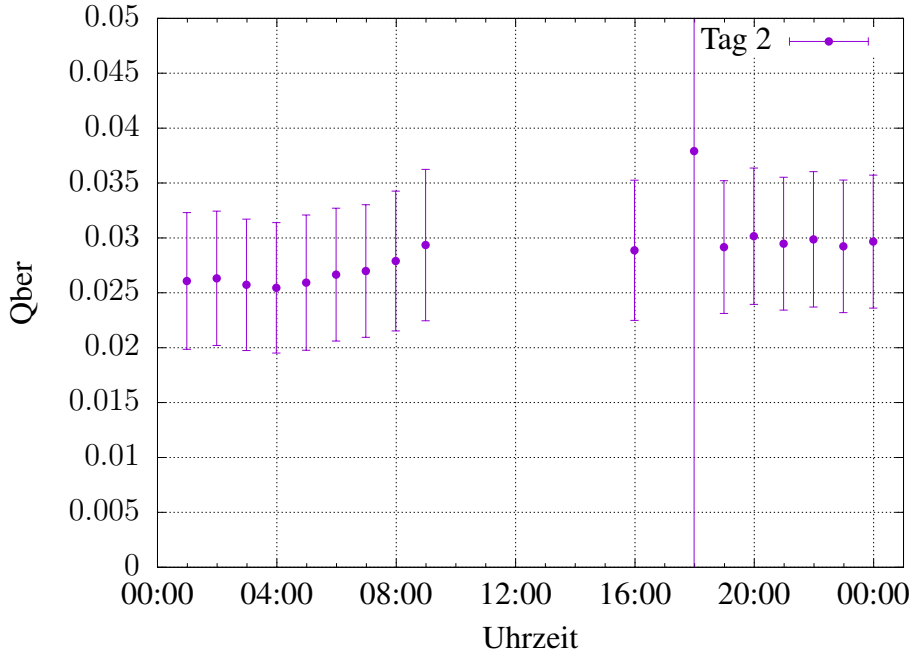

Abbildung B.42: Tag 2 - Qber - Messung 2

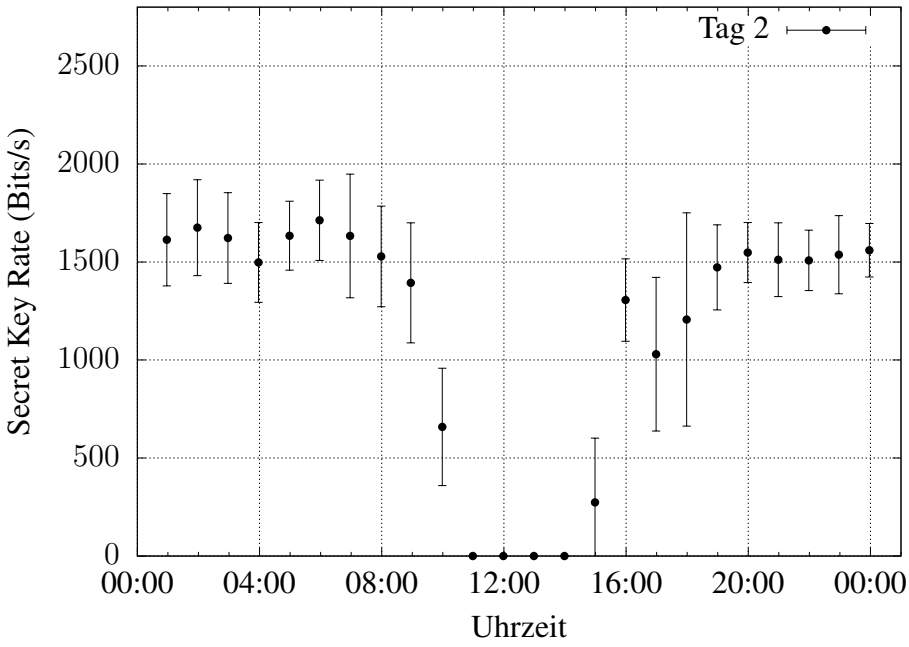

Abbildung B.43: Tag 2 - Secret Key Rate - Messung 2

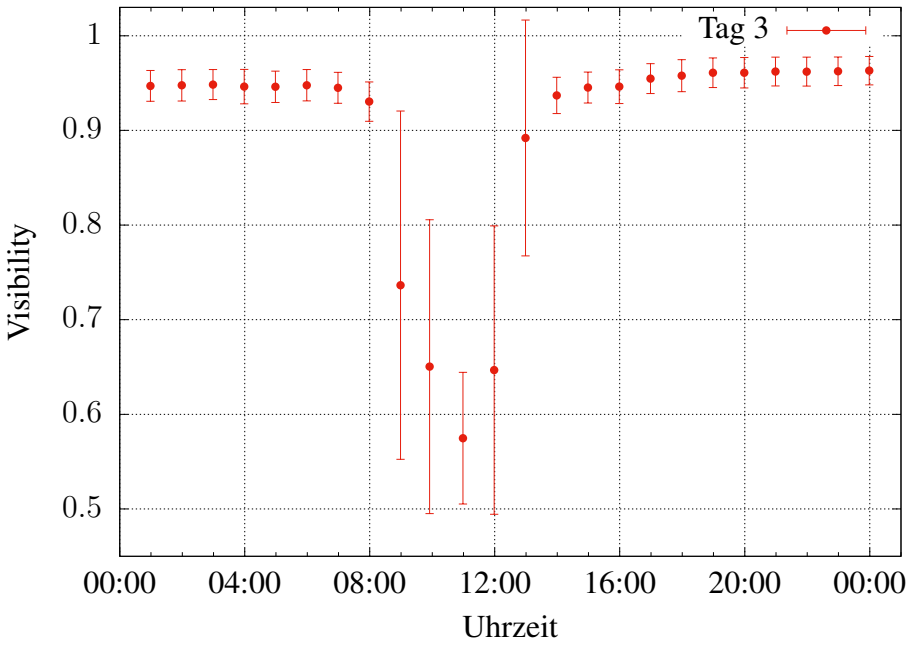

Abbildung B.44: Tag 3 - Visibility - Messung 2 - Erweiterter y-Achsenbereich

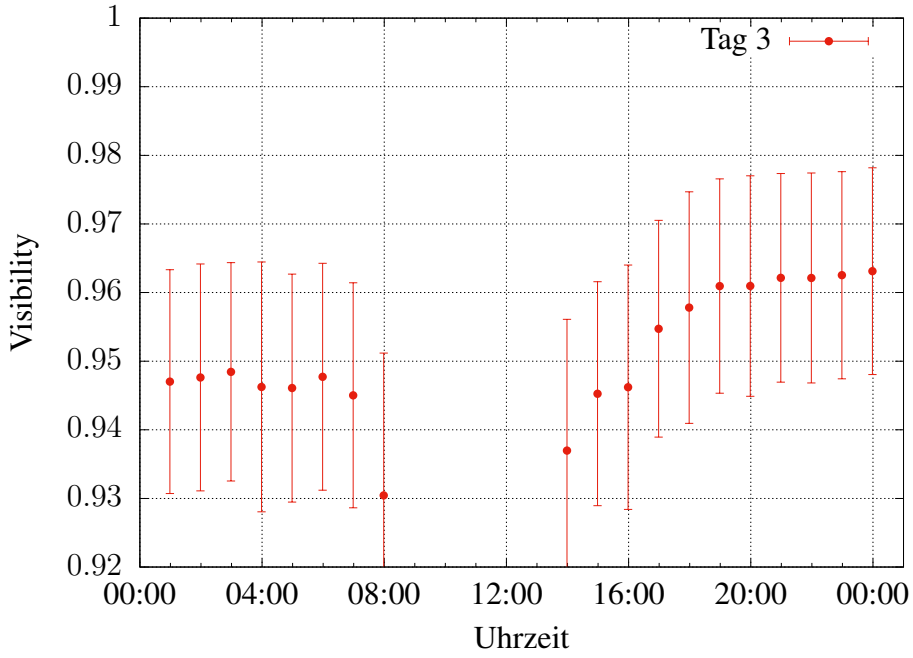

Abbildung B.45: Tag 3 - Visibility - Messung 2

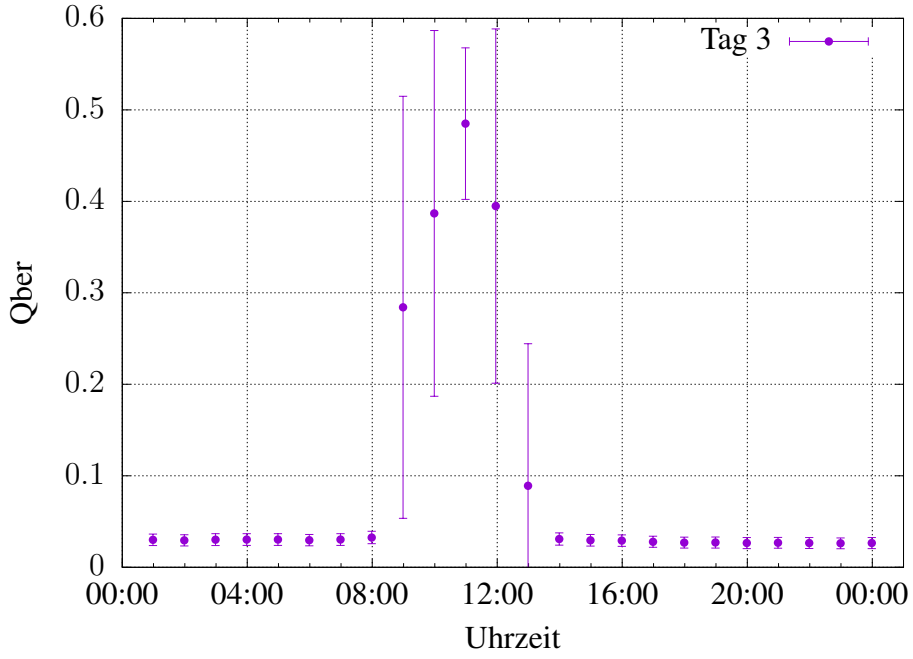

Abbildung B.46: Tag 3 - Qber - Messung 2 - Erweiterter y-Achsenbereich

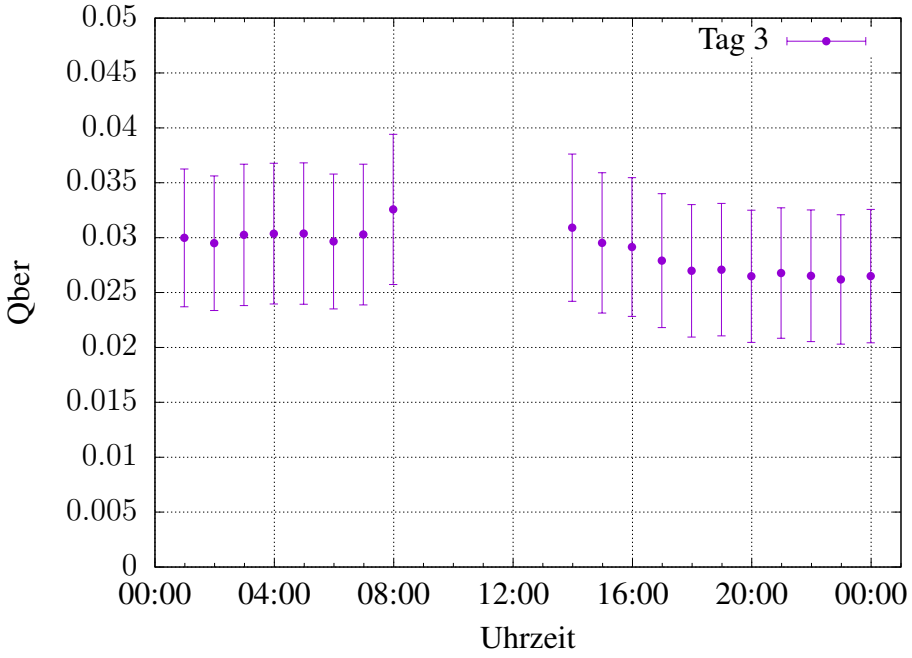

Abbildung B.47: Tag 3 - Qber - Messung 2

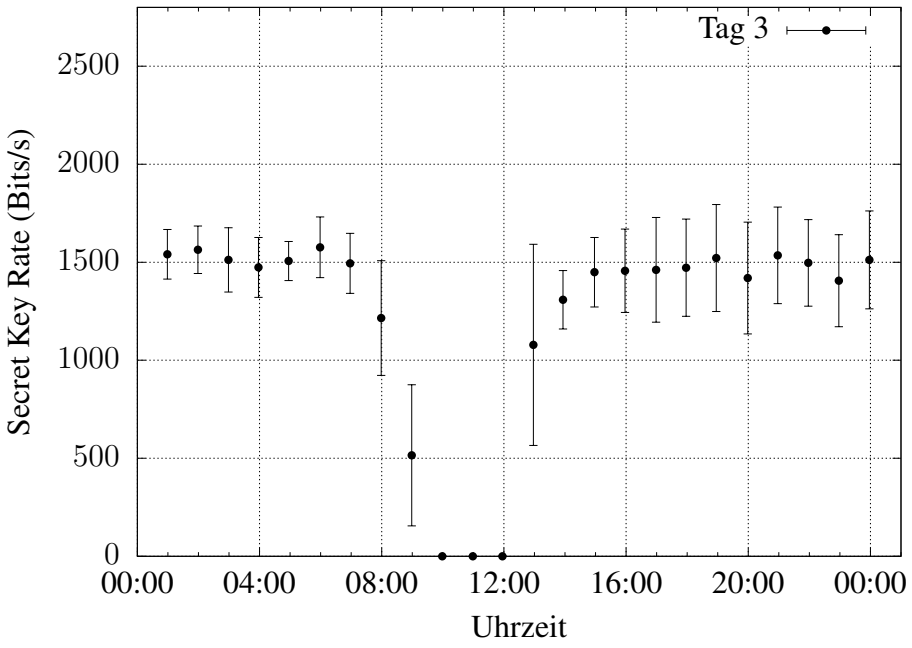

Abbildung B.48: Tag 3 - Secret Key Rate - Messung 2

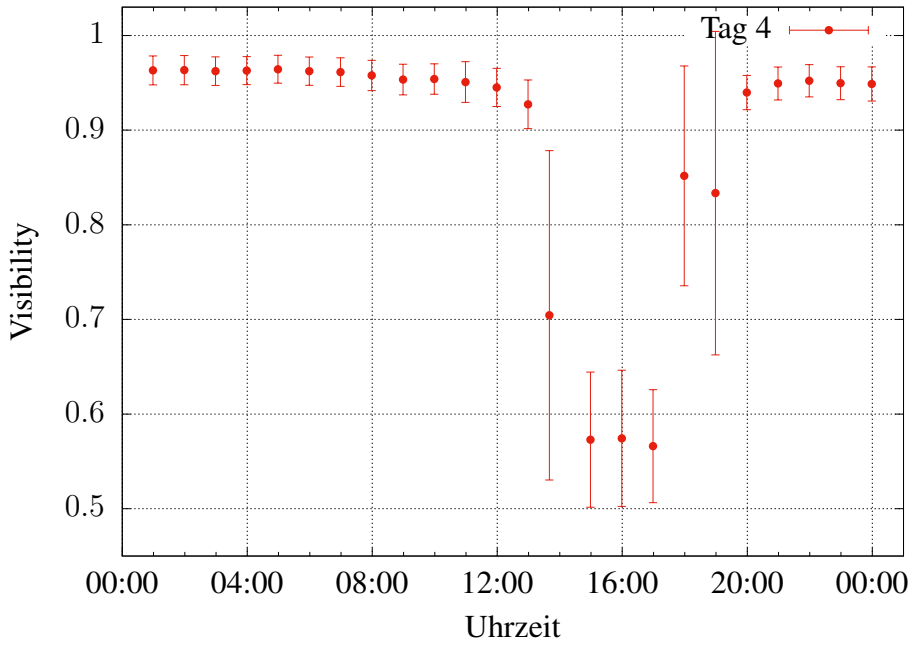

Abbildung B.49: Tag 4 - Visibility - Messung 2 - Erweiterter y-Achsenbereich

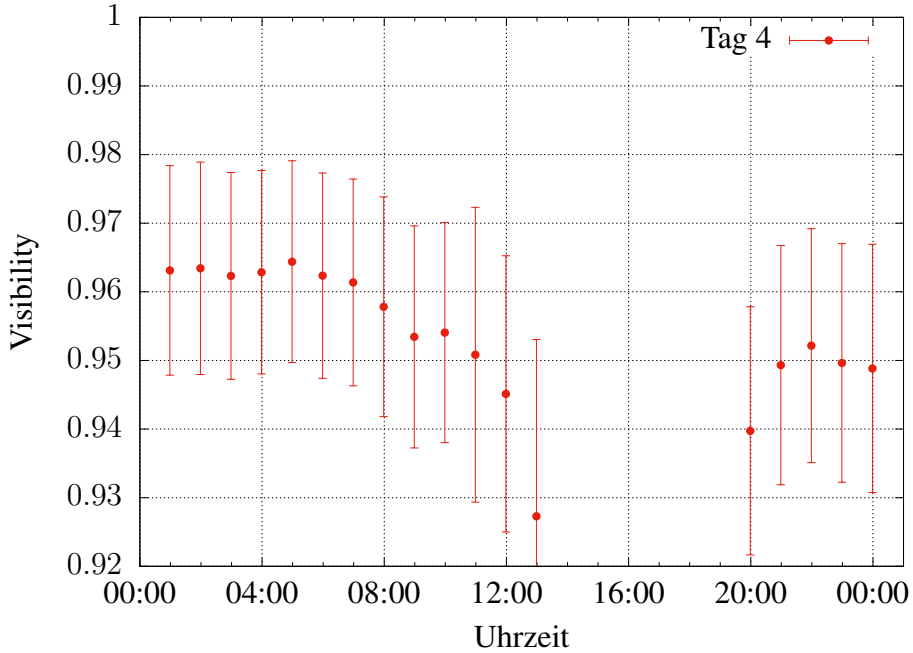

Abbildung B.50: Tag 4 - Visibility - Messung 2

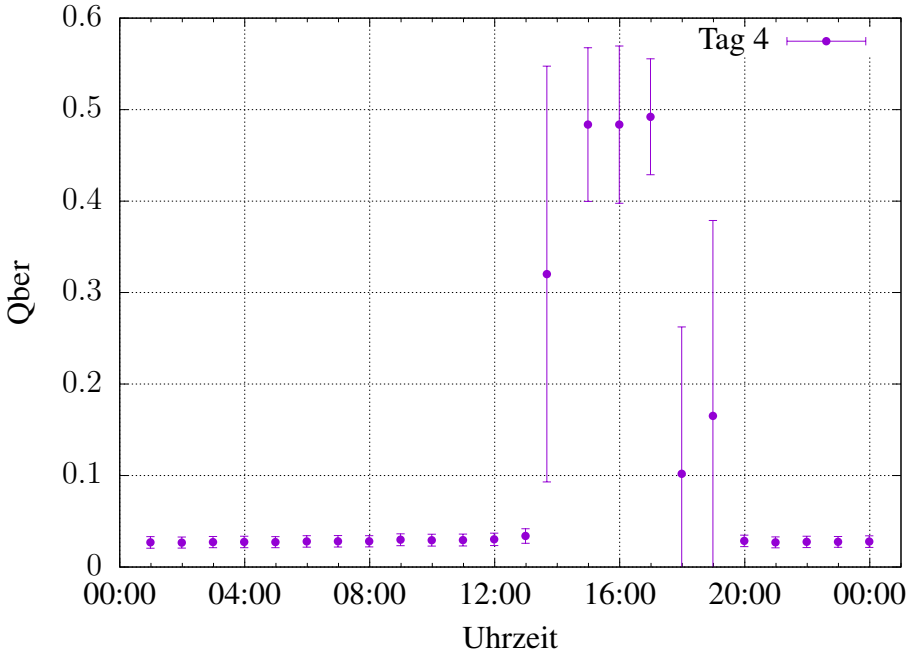

Abbildung B.51: Tag 4 - Qber - Messung 2 - Erweiterter y-Achsenbereich

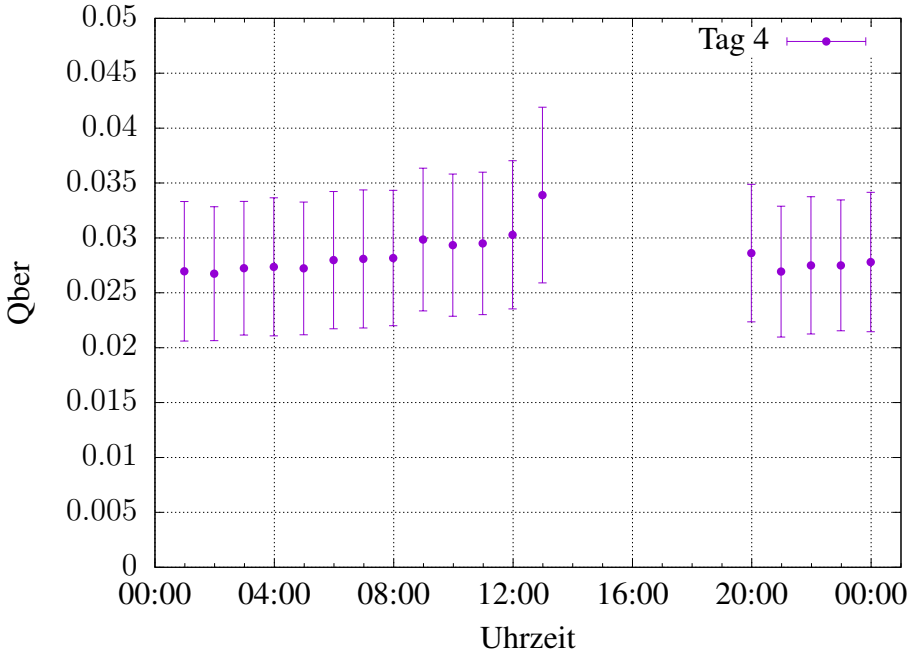

Abbildung B.52: Tag 4 - Qber - Messung 2

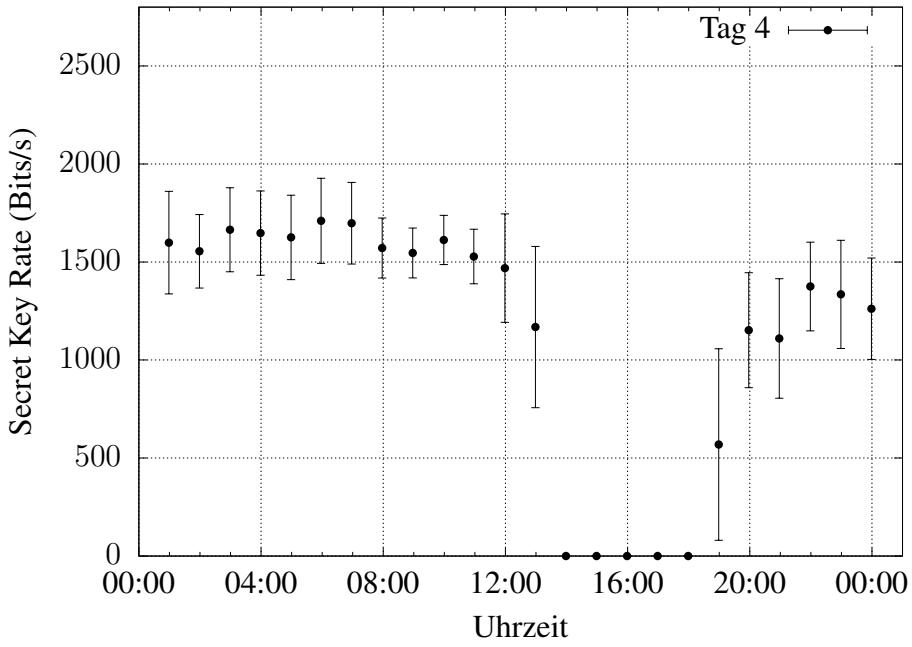

Abbildung B.53: Tag 4 - Secret Key Rate - Messung 2

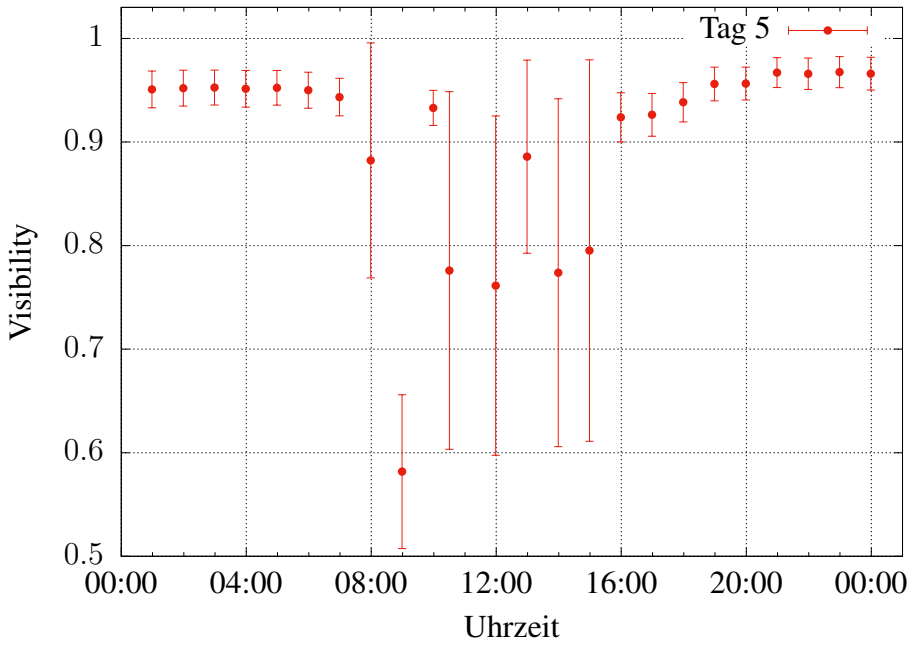

Abbildung B.54: Tag 5 - Visibility - Messung 2 - Erweiterter y-Achsenbereich

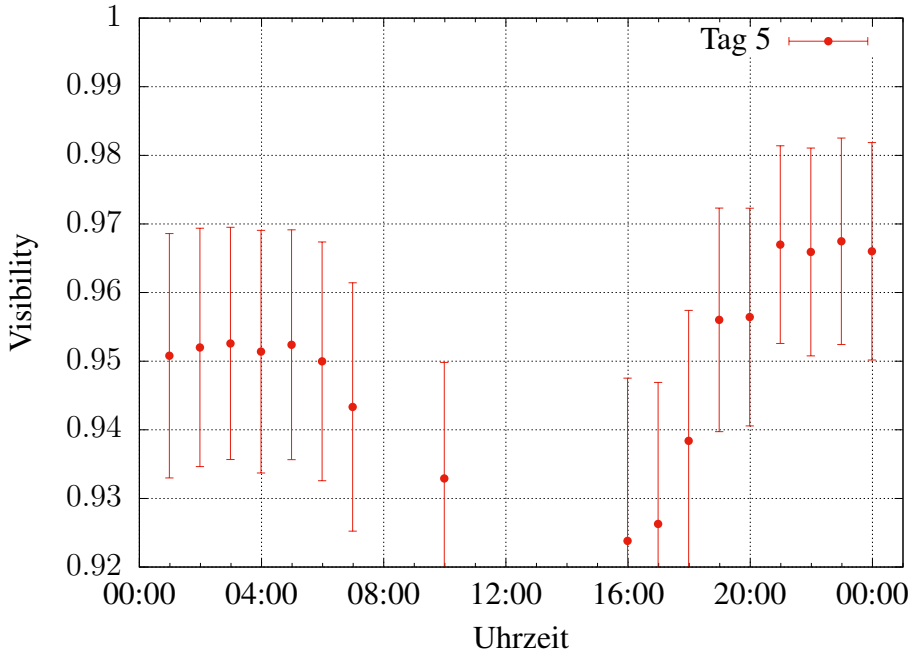

Abbildung B.55: Tag 5 - Visibility - Messung 2

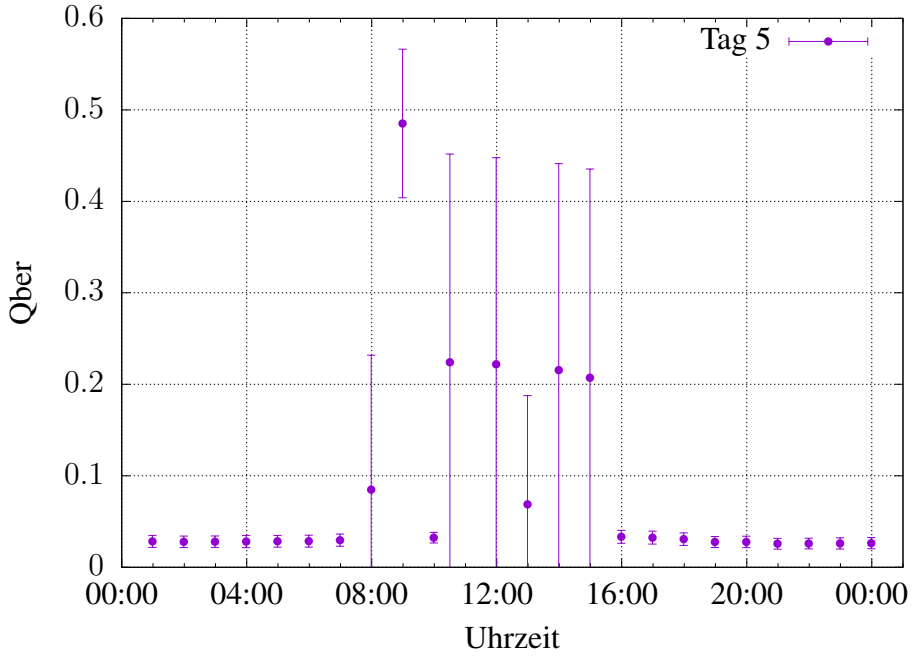

Abbildung B.56: Tag 5 - Qber - Messung 2 - Erweiterter y-Achsenbereich

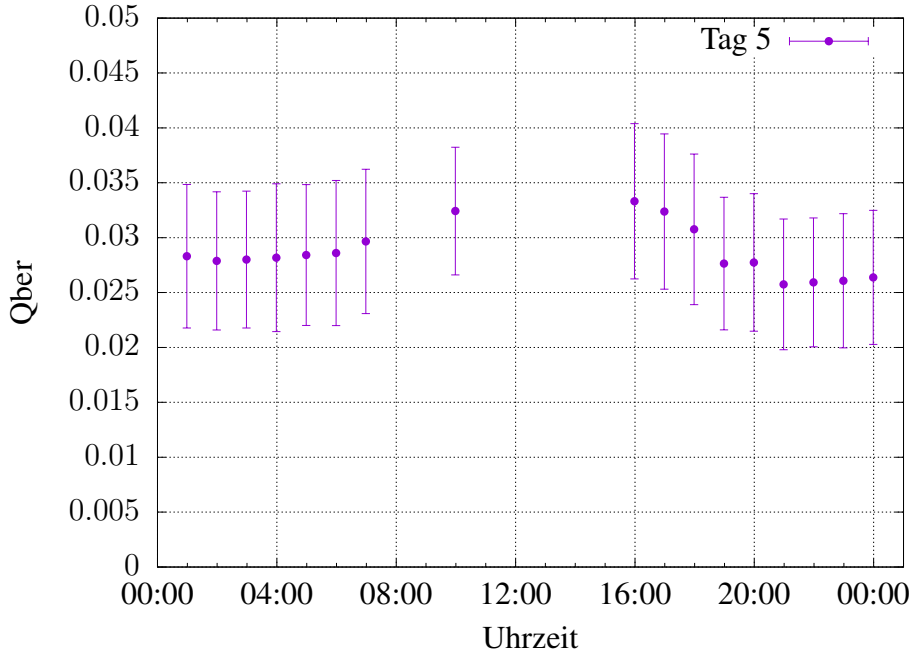

Abbildung B.57: Tag 5 - Qber - Messung 2

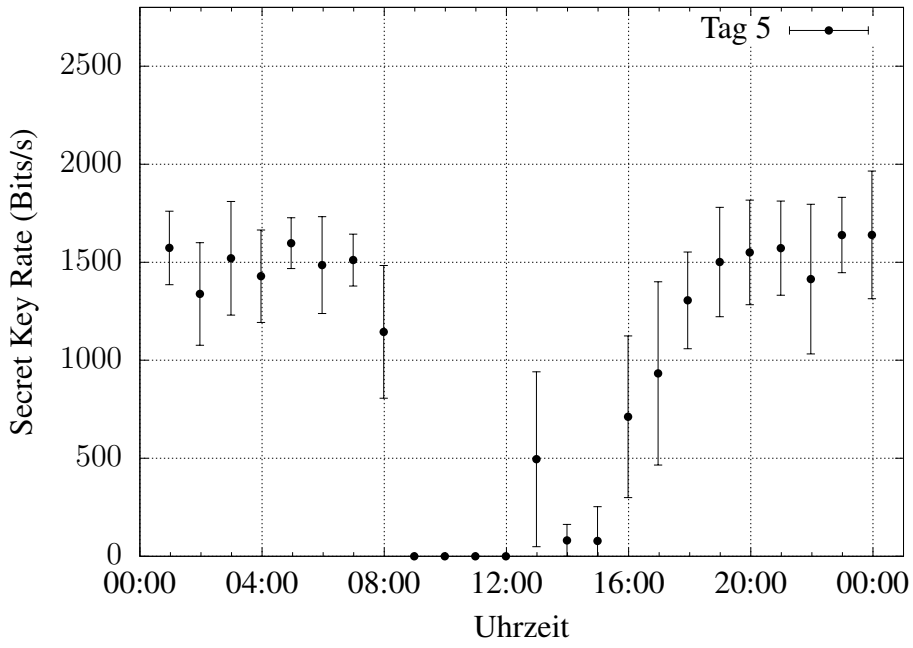

Abbildung B.58: Tag 5 - Secret Key Rate - Messung 2

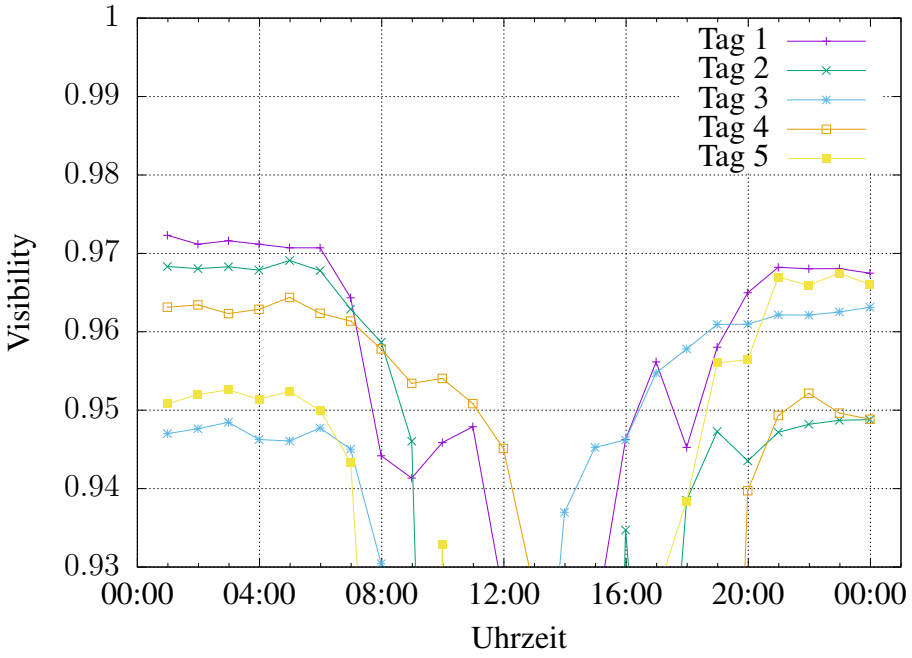

Abbildung B.59: Tag 1-5 - Visibility - Messung 2 - Vergrößert

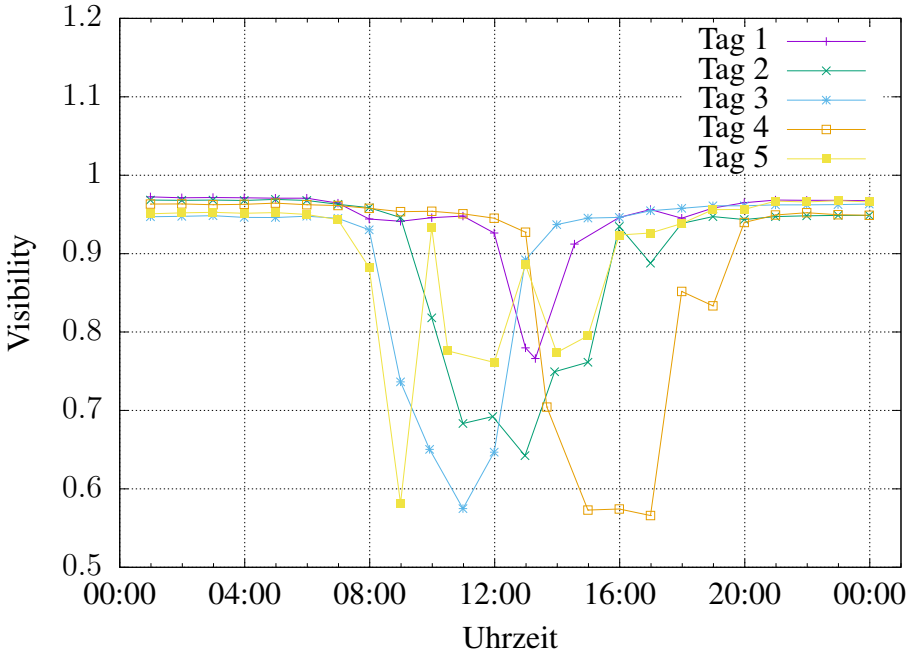

Abbildung B.60: Tag 1-5 - Visibility - Messung 2

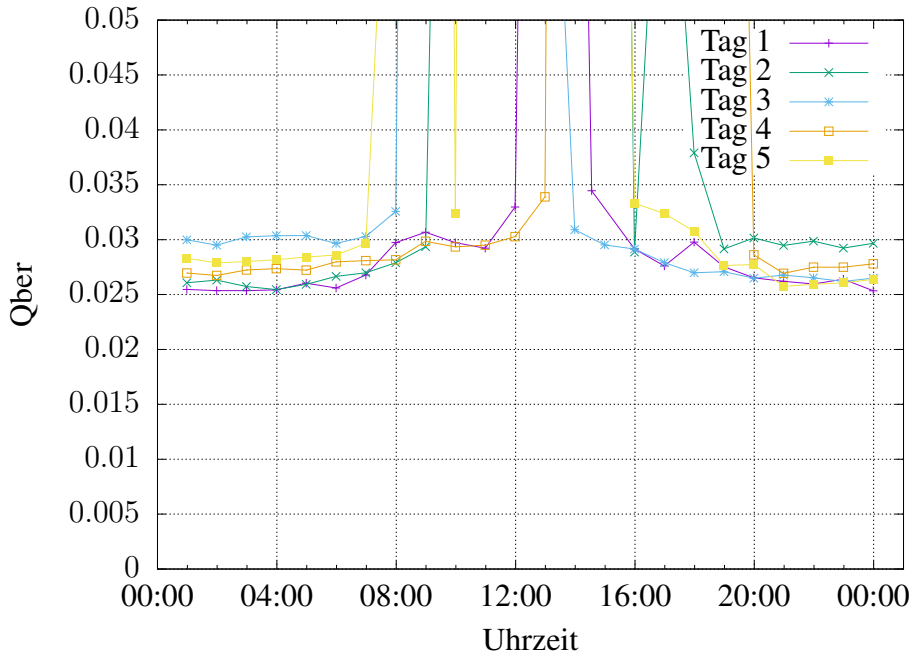

Abbildung B.61: Tag 1-5 - Qber - Messung 2 - Vergrößert

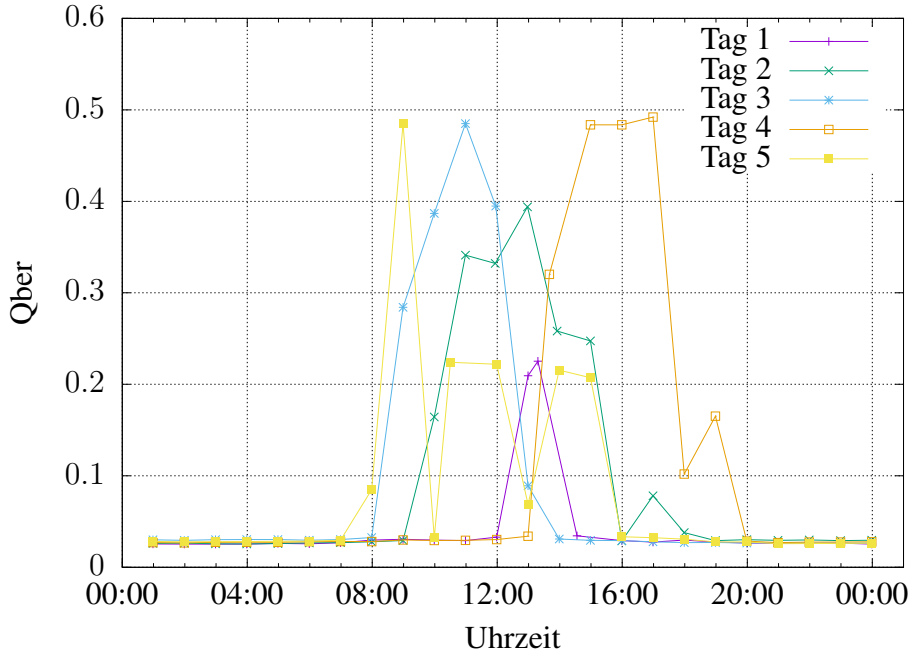

Abbildung B.62: Tag 1-5 - Qber - Messung 2

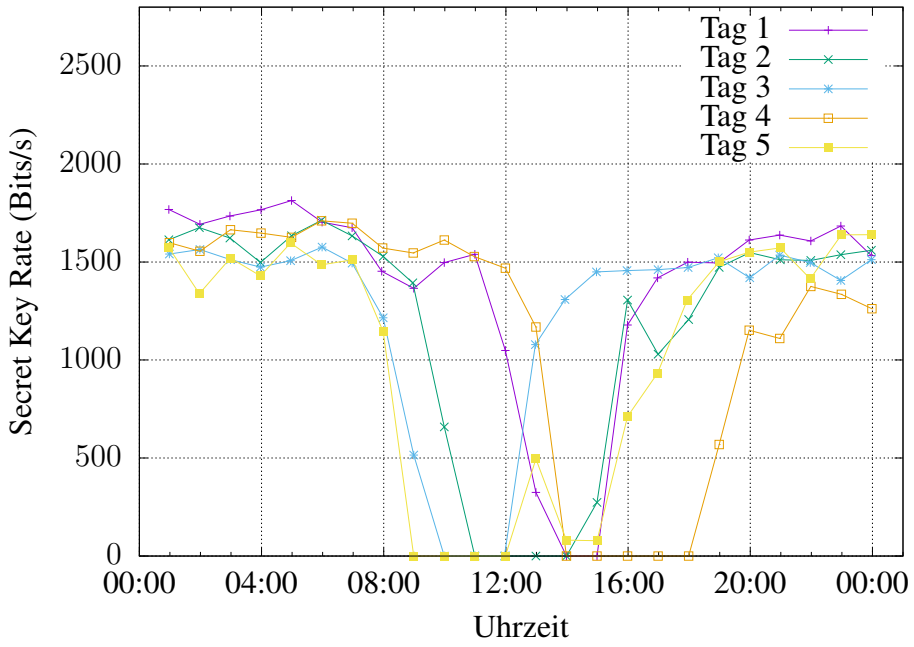

Abbildung B.63: Tag 1-5 - Secret Key Rate - Messung 2

Tabelle B.2: Beobachtete Wetterverhältnisse bei der zweiten Stabilitätsmessung

	00:00 - 03:00	03:00 - 06:00	06:00 - 09:00	09:00 - 12:00
Tag 1	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 2	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 3	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 4	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 5	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt
Tag 6	Nacht	Nacht	Sonnenaufgang	Sonnig, bewölkt

	12:00 - 15:00	15:00 - 18:00	18:00 - 21:00	21:00 - 24:00
Tag 1	Sonnig	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang
Tag 2	Sonnig, bewölkt	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang
Tag 3	Sonnig	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang
Tag 4	Sonnig	Sonnig	Sonnig, bewölkt	Sonnenuntergang
Tag 5	Sonnig	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang
Tag 6	Sonnig, bewölkt	Sonnig, bewölkt	Sonnig, bewölkt	Sonnenuntergang

Anhang C

Einfluss von Tageslicht

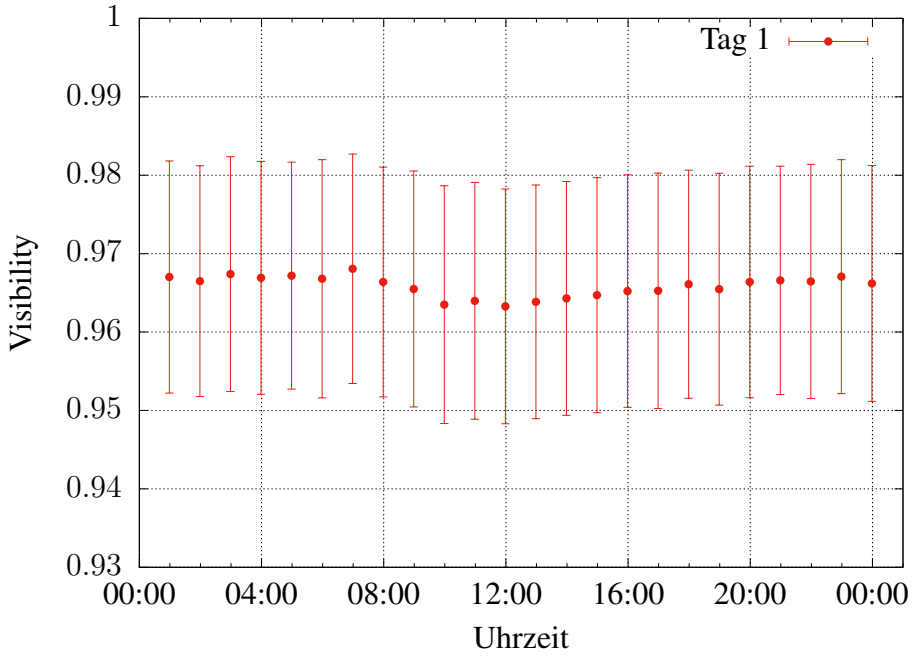

Abbildung C.1: Tag 1 - Visibility - Abgedeckt

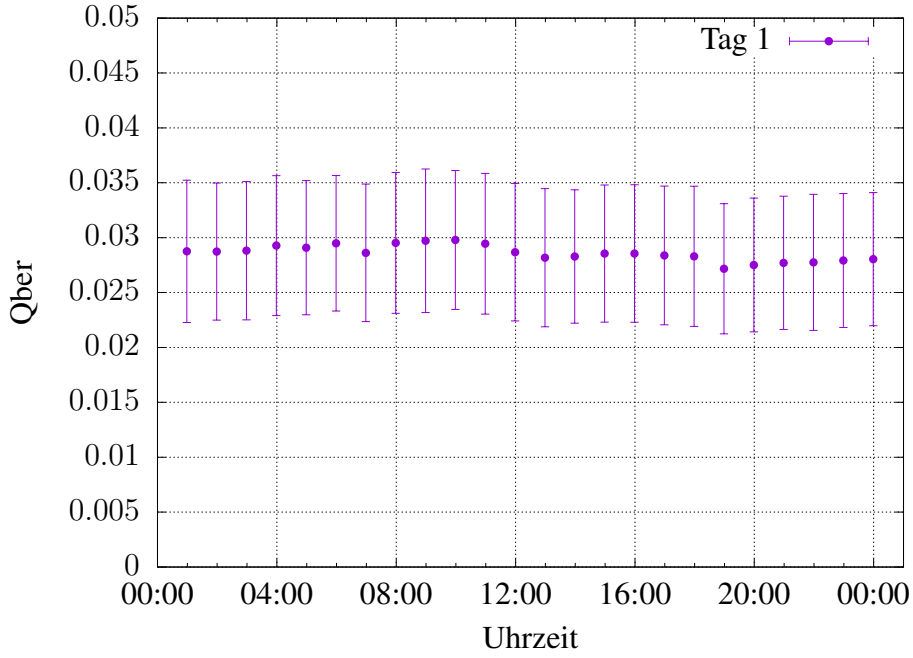

Abbildung C.2: Tag 1 - Qber - Abgedeckt

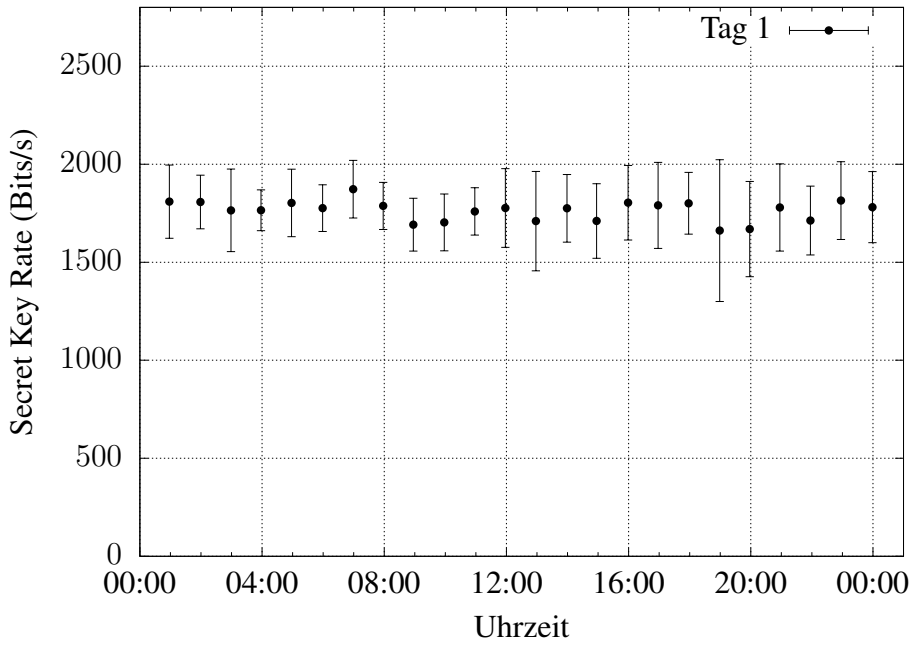

Abbildung C.3: Tag 1 - Secret Key Rate - Abgedeckt

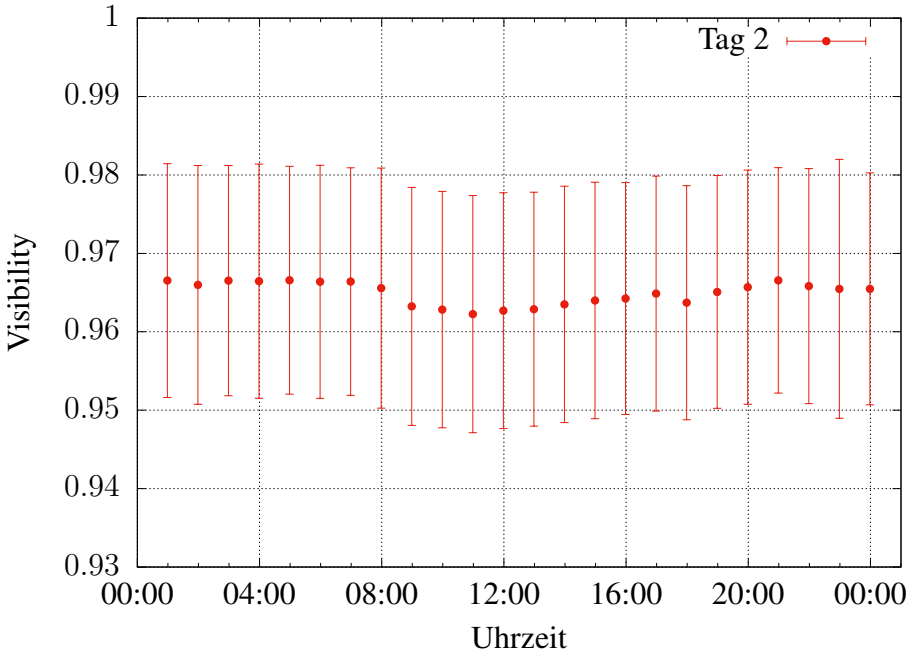

Abbildung C.4: Tag 2 - Visibility - Abgedeckt

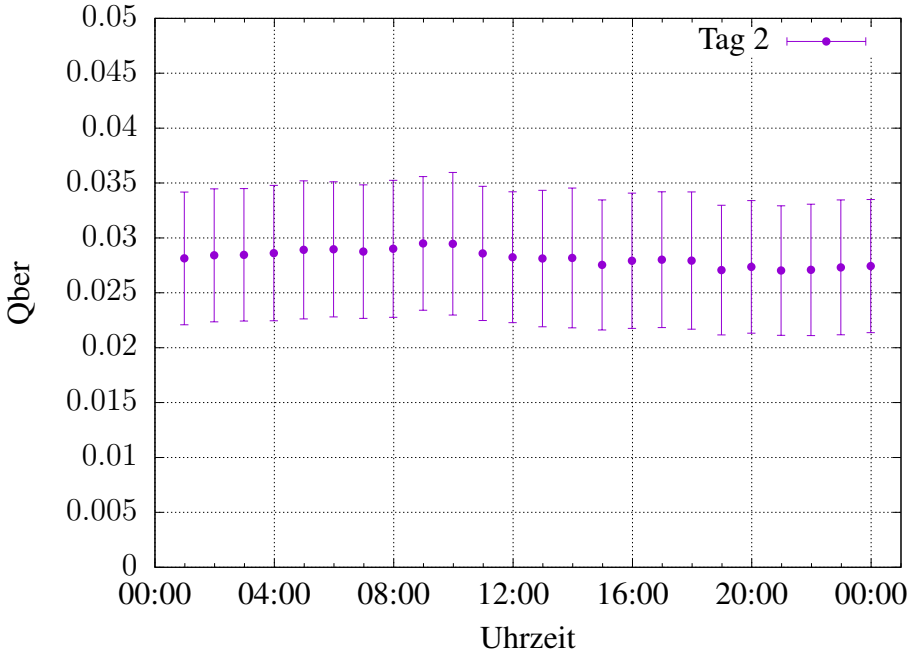

Abbildung C.5: Tag 2 - Qber - Abgedeckt

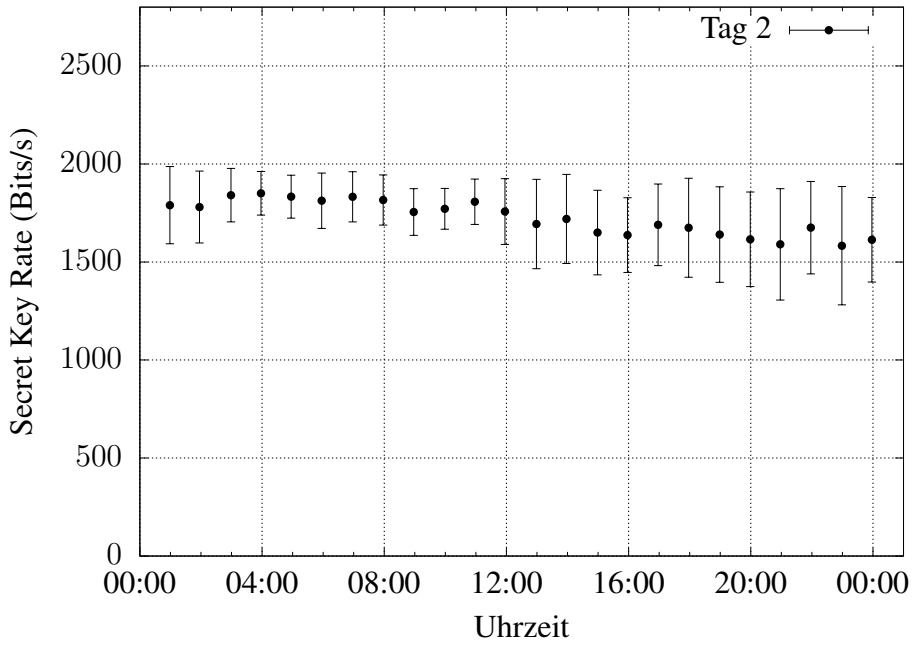

Abbildung C.6: Tag 2 - Secret Key Rate - Abgedeckt

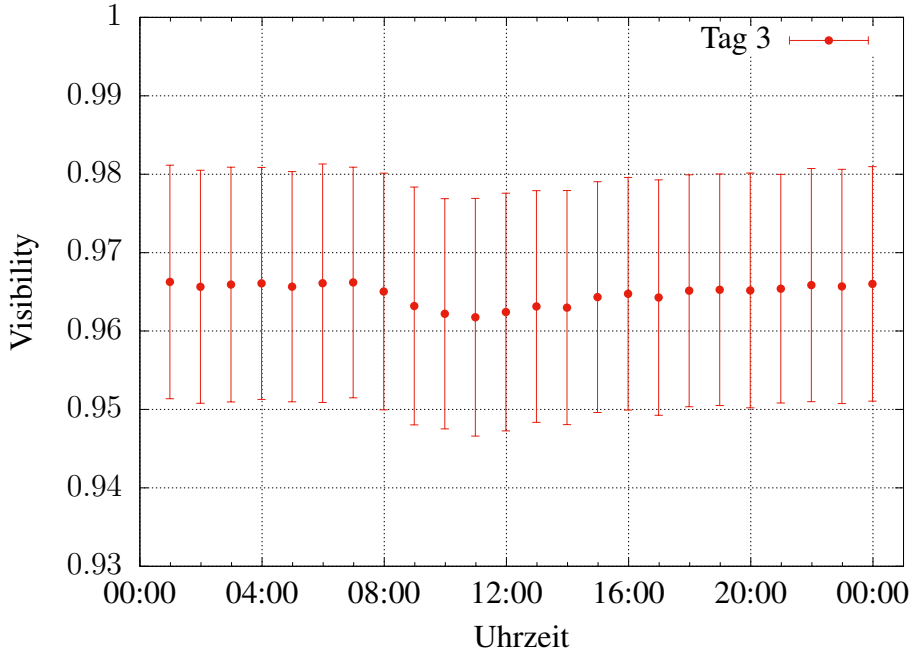

Abbildung C.7: Tag 3 - Visibility - Abgedeckt

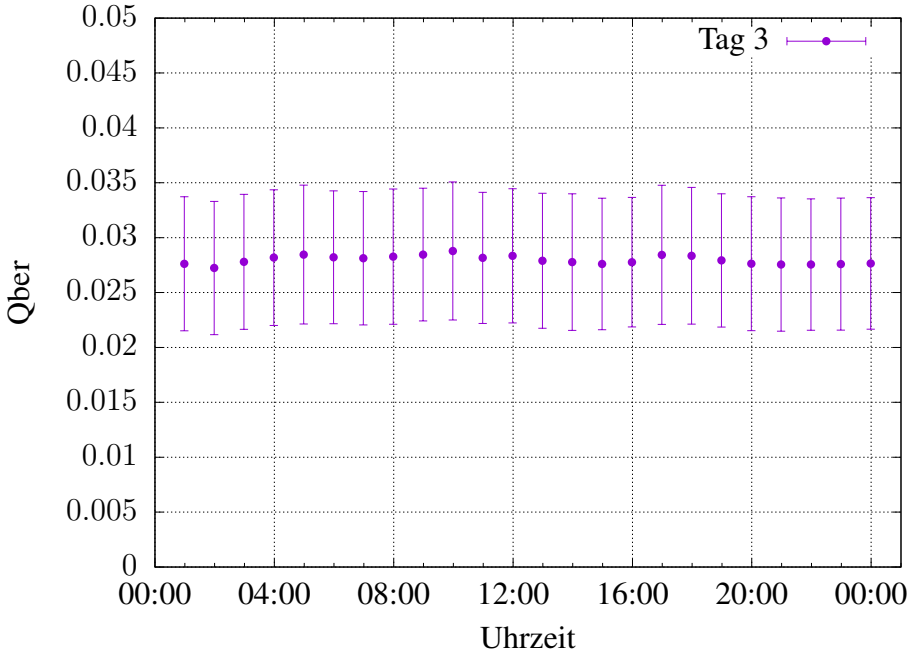

Abbildung C.8: Tag 3 - Qber - Abgedeckt

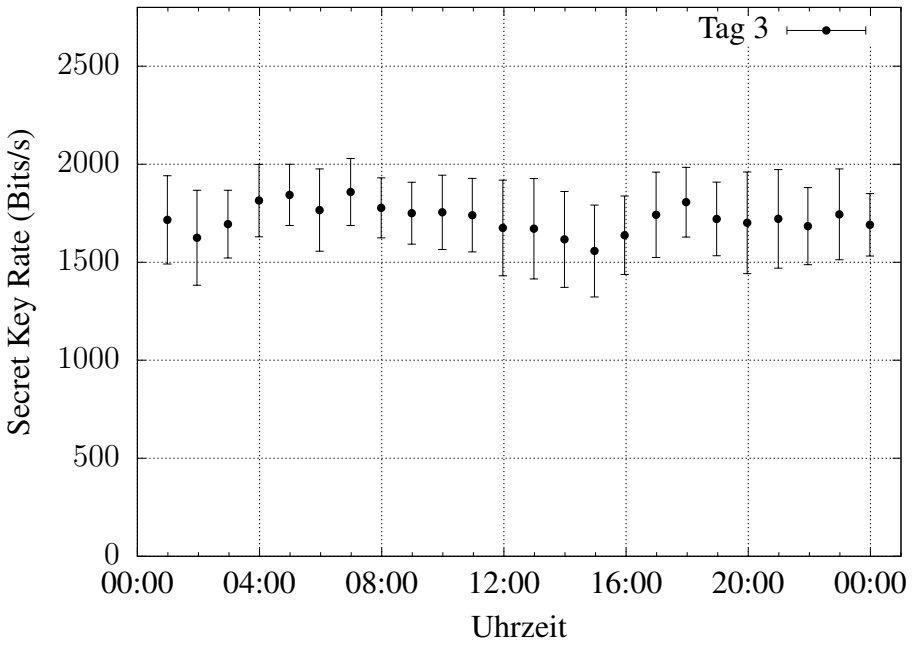

Abbildung C.9: Tag 3 - Secret Key Rate - Abgedeckt

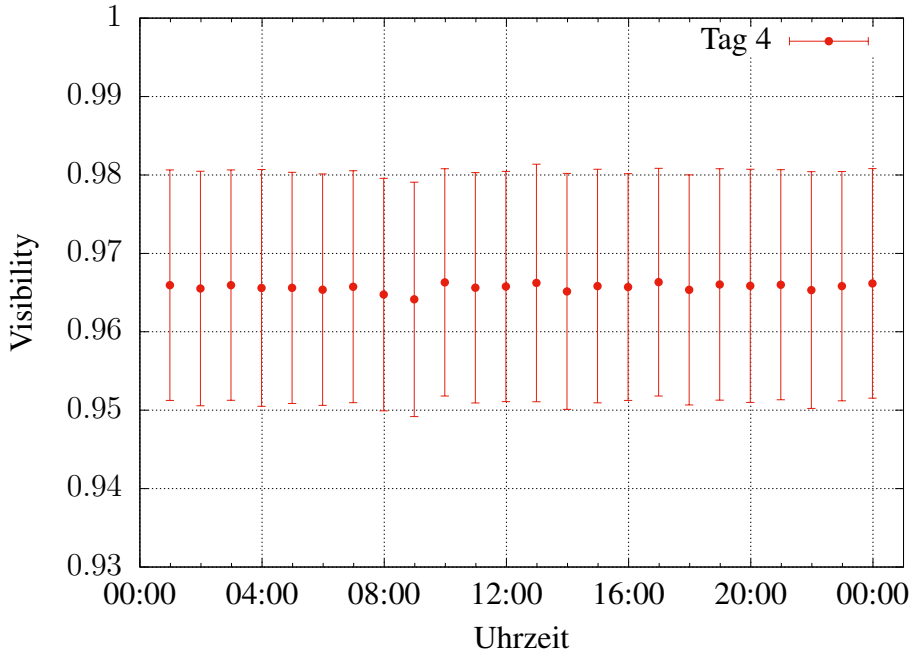

Abbildung C.10: Tag 4 - Visibility - Abgedeckt

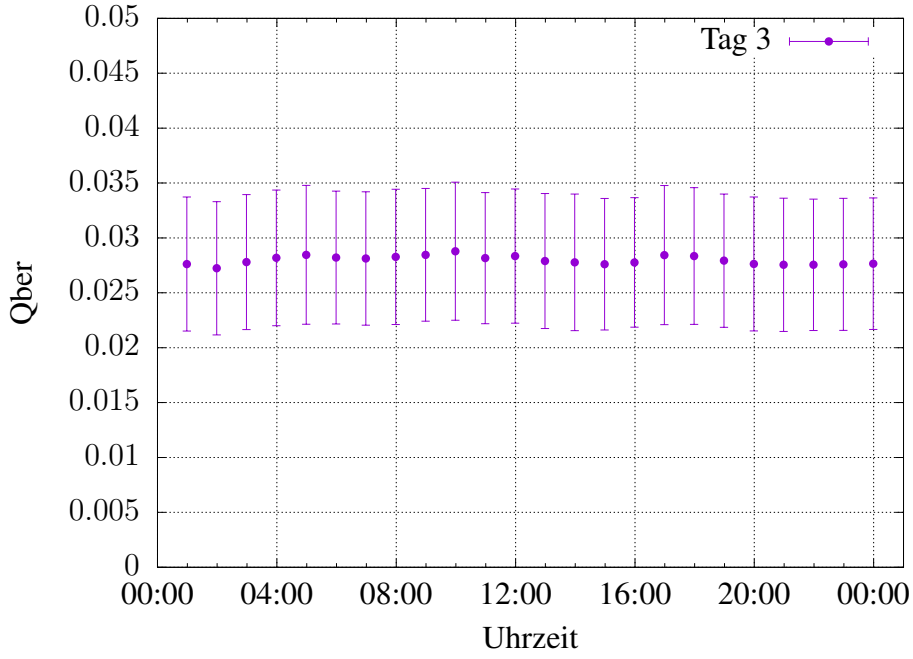

Abbildung C.11: Tag 4 - Qber - Abgedeckt

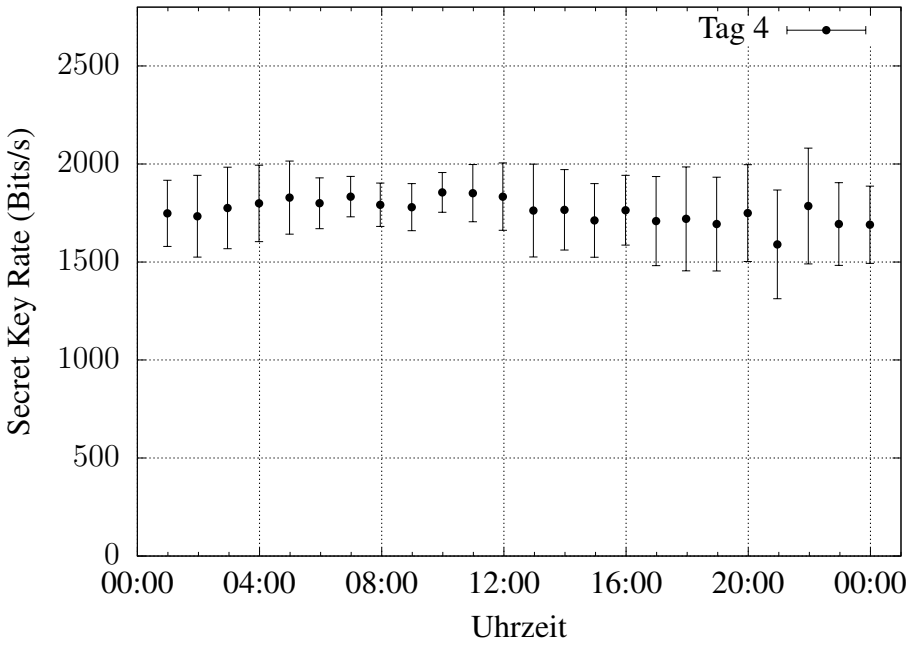

Abbildung C.12: Tag 4 - Secret Key Rate - Abgedeckt

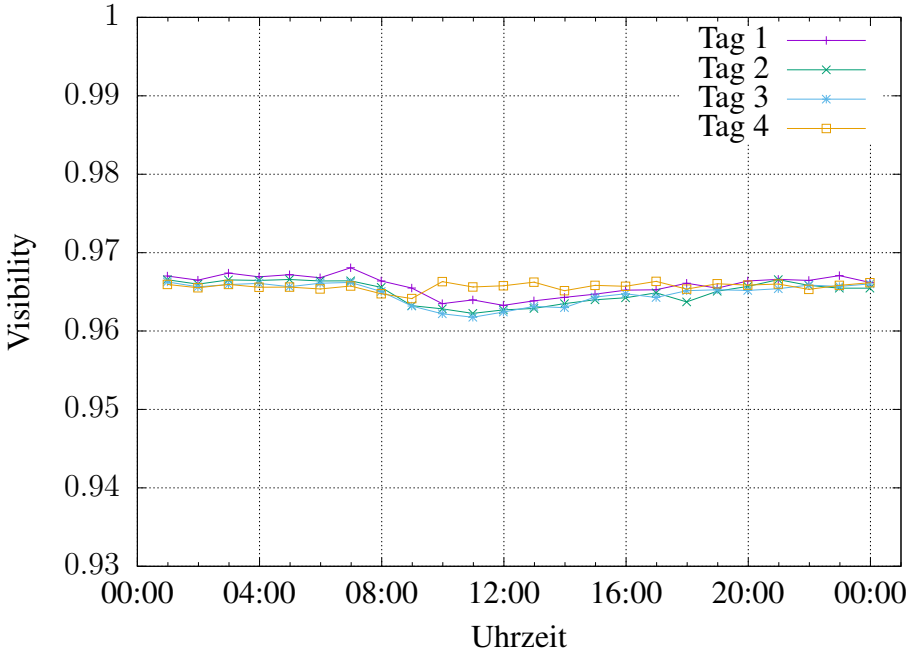

Abbildung C.13: Tag 1-4 - Visibility - Abgedeckt

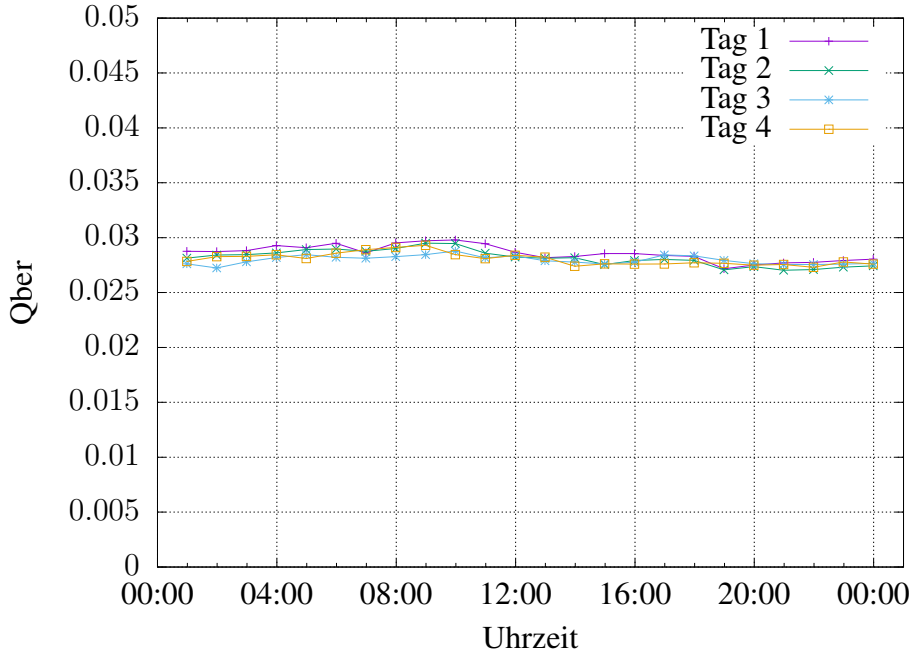

Abbildung C.14: Tag 1-4 - Qber - Abgedeckt

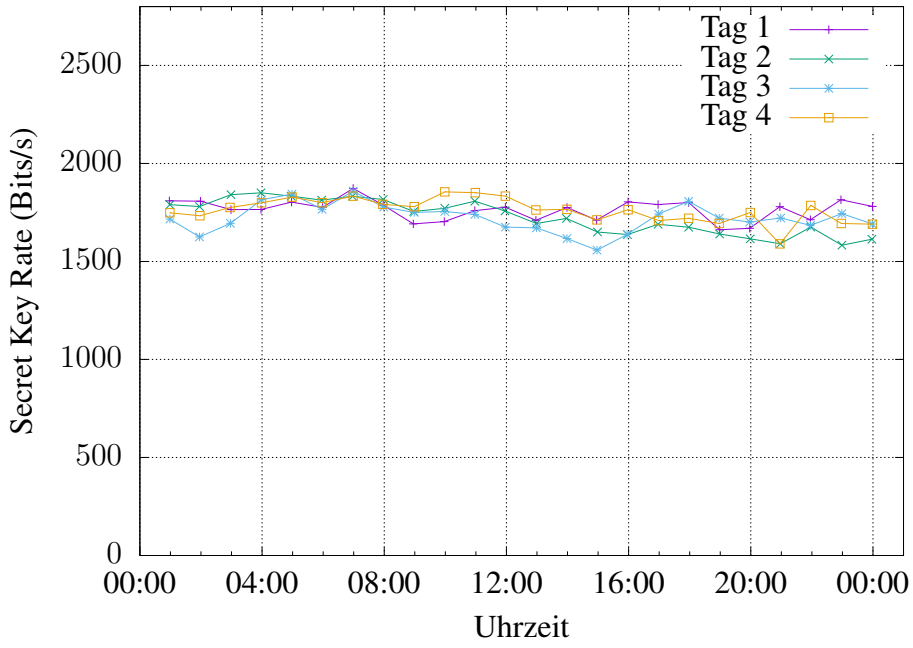

Abbildung C.15: Tag 1-4 - Secret Key Rate - Abgedeckt

Anhang D

Auswirkungen optischer Verluste

D.1 Auswirkungen verschiedener optischer Verluste

Tabelle D.1: Tabelle der benutzten Attenuatoren mit den optischen Dämpfungen, den Stückelungen und den Unsicherheiten

Optische Dämpfung [dB]	Stückelung [dB]	Unsicherheit [± dB]
4	3 + 1	0,5 + 0,5
5	5	0,5
6	6	0,5
7	7	0,5
8	7 + 1	0,5 + 0,5
9	7 + 2	0,5 + 0,5
10	10	1
11	10 + 1	1 + 0,5
12	12	1,2
13	12 + 1	1,2 + 0,5
14	12 + 2	1,2 + 0,5
15	15	1,5

Anhang E

Dense Wavelength Division Multiplexing

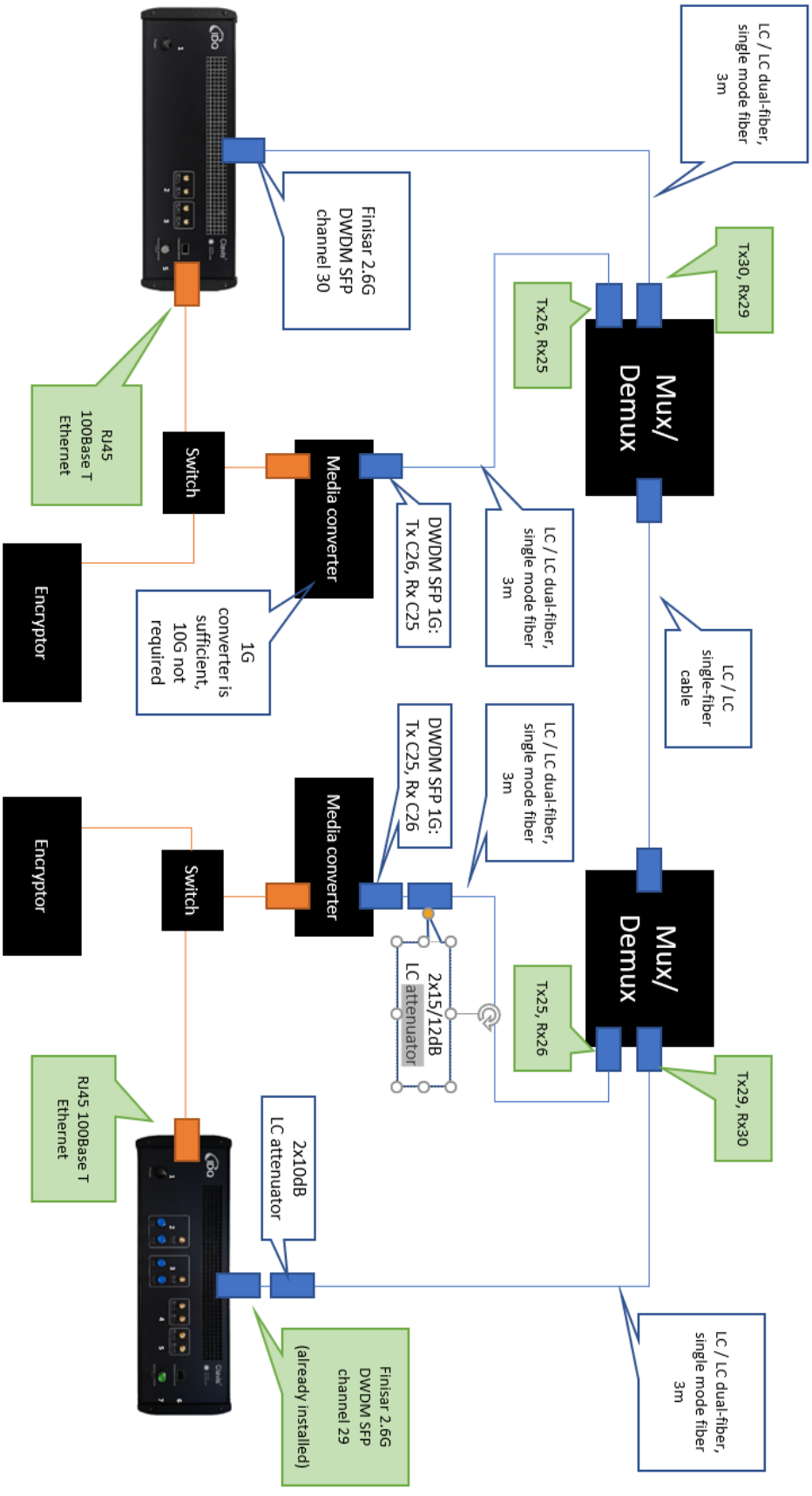

Abbildung E.1: Schematischer Versuchsaufbau mit Dense Wavelength Division Multiplexing [12]

Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt wurden.

Ferner habe ich vom Merkblatt über die Verwendung von Bachelor/Masterabschlussarbeiten Kenntnis genommen und räume das einfache Nutzungsrecht an meiner Bachelor/Masterarbeit der Universität der Bundeswehr München ein.

Neubiberg, 30.06.2021

Ort, Datum

Unterschrift