STORMSHIELD

MEINUNGEN

CYBERSICHERHEIT UND QUANTEN: VORSICHT VOR VEREINFACHUNGEN

Fabien Thomas
Chief Technology Officer,
Stormshield

Quantum System One bei IBM, Quantum AI bei Google, Azure Quantum bei Microsoft, Qian Shi bei Baidu ... Seit Ende der 2010er-Jahre gewinnt das Quantencomputing immer mehr an Bedeutung, sowohl was den Schutz als auch die Bedrohungen für die IT-Sicherheit betrifft. Denn auf lange Sicht könnte diese IT-Revolution tatsächlich Sicherheitssysteme, die auf Verschlüsselung basieren, erheblich schwächen – das heißt, fast alle ... Die Quantenbedrohung – eine neue Herausforderung für die Cybersicherheit. Vorausgesetzt, man versteht das Phänomen richtig und vermeidet vorgefasste Meinungen.

Vorwort: Um die Lesbarkeit dieses Papiers zu erhalten, werden wir hier nicht detailliert auf die Algorithmen von Grover und Shor eingehen oder auf alle Schattierungen von Qubits (stable, *noisy, annealing* und die anderen ...). Es geht auch um die geistige Gesundheit unserer Leserinnen und Leser.

DIE VERHEISSUNGEN DER QUANTENRECHENLEISTUNG

Vom traditionellen Computer zum Quantencomputer

Quantencomputer sind zwar faszinierend, aber auch äußerst kompliziert zu verstehen. Und hinter dem Lack verbergen sich in Wirklichkeit viele Unsicherheiten – zusammengefasst mit dem berühmten Zitat, das dem Physiker Richard Feynman zugeschrieben wird: *„Ich glaube, ich kann mit Sicherheit sagen, dass niemand die Quantenmechanik versteht."* Ein Paradigma, das Sie bei der Lektüre dieses Papiers im Hinterkopf behalten sollten. *„wenn es um Quanten geht, sollte man nicht versuchen, sie intuitiv zu verstehen"*, ergänzt **Yvan Vanhullebus**, Technical Leader bei Stormshield. *Denn unsere Intuition beruht auf unseren bisherigen Erfahrungen und ist überhaupt nicht quantentrainiert. So sehr, dass es heute einfacher zu sein scheint, zu erklären, was die Quanten NICHT sind ..."*

„Wenn es um Quanten geht, sollte man nicht versuchen, sie durch Intuition zu verstehen. Denn unsere Intuition beruht auf unseren bisherigen Erfahrungen und ist überhaupt nicht quantentrainiert. So sehr, dass es heute einfacher zu sein scheint, zu erklären, was die Quanten NICHT sind ..."

Yvan Vanhullebus, Technical Leader bei Stormshield

Ein kompliziertes Thema, das vor allem die Welt der Cybersicherheit begeistert, da **das Quantencomputing die Informatik, wie wir sie heute kennen, revolutionieren könnte.** Wie ist das möglich? Durch den „Quantensprung", d. h. die Möglichkeit, von einer optimierten Rechenleistung zu profitieren und so komplexe mathematische Operationen durchführen zu können, die bisher nicht möglich waren. Wie Yvan Vanhullebus erklärt: *„Der Quantencomputer nutzt die Eigenschaften der Materie auf einer unendlich kleinen Skala, um in wenigen Minuten bestimmte Berechnungen durchzuführen, die mit dem leistungsfähigsten heutigen Computer mindestens mehrere tausend Jahre dauern würden."*

Die Quanteninformatik ist eng mit einer neuen Einheit verbunden: dem Quantenbit oder „Qubit". Eine Einheit, die, wie in den meisten Artikeln erklärt, zwei Werte annehmen kann (die mit 0 oder 1 bezeichnet werden), die aber auch beide Werte gleichzeitig annehmen kann, sodass alle Werte gleichzeitig berechnet werden können. ***„Aber in Wirklichkeit funktioniert es nicht so: Man ist näher an der Quantenrealität, wenn man von Wahrscheinlichkeiten spricht"***, wie Yvan Vanhullebus erklärt, der auf einen ... Comic als Referenzdokument zu diesem Thema verweist: den Cartoon *„The Talk"* von Scott Aaronson und Zach Weinersmith.

Gewünschte Anwendungen von Quantencomputern

Zahlreiche Akteure haben sich auf ein regelrechtes technologisches Wettrennen eingelassen, um die Quantenvorherrschaft zu erreichen. **Aber was ist Quantensuprematie?** Dies ist der Zeitpunkt, an dem eine Quantenberechnung zu einem bestimmten Problem schneller ist als ihr Computeräquivalent. Auch wenn einige Akteure regelmäßig erklären, dass sie diese Quantenvorherrschaft erreicht haben, lässt der Umschwung in die eigentliche Ära des Quantencomputings noch auf sich warten. In diesem Rennen um den Supercomputer gab es daher zahlreiche Ankündigungen von privaten Akteuren wie Google, IBM oder Baidu, die jeweils ausführlich über ihre (mehr oder weniger experimentellen) Fortschritte in diesem Bereich berichteten. Wer hat also **die Quantenvorherrschaft erreicht?** Unter den Experten des Themas gibt es keinen Konsens, insbesondere sind nicht alle Qubits gleich ... Die Qubit-Mengen der verschiedenen Ankündigungen können manchmal überraschen – denn sie bedeuten nicht immer das Gleiche ... Bereits 2019 gab Google bekannt, diese Quantenvorherrschaft erreicht zu haben, vor chinesischen Forschern im Jahr 2021 – aber in beiden Fällen wurden die Ergebnisse angezweifelt. Zwischen den 54 Qubits des Sycamore-Prozessors von Google und den 433 für den Osprey-Prozessor von IBM ist der Qubit-Wettbewerb eröffnet und in vollem Gange.

Die öffentlichen Akteure stehen in diesem technologischen Wettlauf nicht zurück. In den USA interessiert sich die NSA schon seit Jahren für den Quantensektor (2014 gab sie ihre ersten 80 Millionen Dollar für ein Programm mit dem Titel *Owning The Net* aus). Europa seinerseits plant, bis 2027 mindestens 4,5 Milliarden Euro in Quantentechnologien zu investieren. Die französische Regierung hat ihrerseits im Januar 2021 einen Betrag von 1,8 Milliarden Euro für Quantentechnologien bereitgestellt. „*Ein nicht unerhebliches Budget, aber weniger als die chinesischen und amerikanischen Investitionen*", schränkt **Noël Chazotte**, Product Manager bei Stormshield, ein. *Wenn man bedenkt, dass die genannten Beträge in den USA bei 25 Milliarden Dollar und in China bei 50 Milliarden Dollar liegen, bewegt sich Europa nicht auf derselben Skala ...*"

„Europa plant, bis 2027 mindestens 4,5 Milliarden Euro in Quantentechnologien zu investieren. Die französische Regierung hat ihrerseits im Januar 2021 einen Betrag von 1,8 Milliarden Euro für Quantentechnologien bereitgestellt."

Denn es steht viel auf dem Spiel: Es geht darum, eine Technologie zu beherrschen, die als revolutionär angepriesen wird. Die Funktionsweise des Universums oder das Verhalten von Materie auf molekularer Ebene zu simulieren, neue bewohnbare Planeten zu finden, das Wetter besser vorherzusagen, Medikamente zu entwickeln, die große Krankheiten wie Krebs oder Alzheimer behandeln können, aber auch Bankbetrug zu bekämpfen und insgesamt die Sicherheit von Informationssystemen zu verbessern ... Die Anwendungen sind vielfältig und betreffen zahlreiche Industriezweige. Doch während die Versprechungen dieser Industrie beeindruckend sind, **stellt das Quantencomputing auch eine neue Bedrohung für die Cybersicherheitsbranche dar.**

NEUE BEDROHUNGEN, DIE DURCH QUANTENCOMPUTER EINGEFÜHRT WERDEN

Eine Cyberbedrohung ... von staatlicher Seite?

Bevor man den Meldungen Glauben schenkt, die von einer cyberkriminellen Quantenbedrohung sprechen, könnte die Bedrohung vor allem eine geopolitische Wendung nehmen. *„Ganz klar, der erste Staat, der das Rennen um die Beherrschung der Quantentechnologie gewinnt, wird eine Vormachtstellung gegenüber den anderen haben"*, sagt **Arnaud Dufournet**, Chief Marketing Officer von TheGreenBow. *So wie es Atommächte gibt, wird es auch Quantenmächte in der Welt geben. Heute spielt sich dies zwischen China und den USA ab. Zweitens wird es noch länger dauern, bis nichtstaatliche Cyberkriminelle über diese Waffe verfügen.*" **Würde der Quantencomputer dann zu einem neuen Hebel für Industrie- und Staatsspionage oder gar geopolitische Destabilisierung werden?** Es wäre verlockend, mit „Ja" zu antworten, da diese Problematik der nationalen Sicherheit von vielen Ländern sehr ernst genommen wird. In einer seltenen öffentlichen Rede des Leiters des MI6 äußerte der britische Geheimdienst die Sorge, dass einige *„rogue states"*, Schurkenstaaten, sich im Hinblick auf künftige Konflikte im Bereich der Quantentechnik positionieren könnten.

„Ganz klar: Der erste Staat, der den Wettlauf um die Beherrschung der Quantentechnologie gewinnt, wird eine Vorherrschaft über die anderen haben. Ähnlich wie die Atommächte wird es auch Quantenmächte in der Welt geben."

Arnaud Dufournet, Chief Marketing Officer TheGreenBow

Diese latente Bedrohung bzw. die böswillige Nutzung von Quanten liegt im Angriff auf die Schlüssel der asymmetrischen Verschlüsselung begründet. Sie würde zum Zusammenbruch aller Informationssysteme führen, die auf Verschlüsselung beruhen, und trägt sogar den Namen *„Quantenapokalypse"*, ein Ausdruck aus einem Artikel eines *BBC-Berichts*, der vielfach weiterverbreitet wurde. Worum geht es? Auf der Seite der Unternehmen stellen Sie sich vor, dass die Sicherheit Ihrer Informationssysteme von einem Tag auf den anderen nicht mehr gewährleistet ist. Eine reale Aussicht, wie **Ilyas Khan** von der Firma *Quantinuum* und **Harri Owen** von der Firma Post Quantum in Interviews mit der BBC berichten: *„Alles, was wir heute im Internet tun, von Online-Einkäufen bis hin zu Bankgeschäften, ist verschlüsselt. Aber sobald ein funktionierender Quantencomputer in der Lage ist, diese Schlüssel zu knacken, könnte dies die Möglichkeit schaffen, Bankkonten oder Krypto-Wallets zu leeren und außerdem nationale Verteidigungssysteme zum Einsturz zu bringen."*

Eine bereits vorhandene Cyberbedrohung

Doch welcher Art sind die neuen Schwachstellen, die durch den Anbruch des Quantenzeitalters hervorgerufen werden? Sie betreffen fast ausschließlich die Sicherheit kryptografischer Infrastrukturen, die potenziell durch die Rechenleistung von Quanten in Mitleidenschaft gezogen wird, die die derzeitigen asymmetrischen

Kryptografiesysteme (RSA, ECC ...) zum Einknicken bringen könnte. Mit möglichen Folgen wie dem Identitätsdiebstahl von Servern oder anderen am elektronischen Austausch beteiligten Stellen und/oder der Entschlüsselung von Daten. **Bis zu dem Punkt, an dem es möglich ist, einen RSA-2048-Schlüssel in weniger als 24 Stunden zu knacken?** Dies war die Frage, die im *„Quantum Threat Timeline Report"* im Jahr 2021 gestellt wurde, mit einer Projektion auf die nächsten 30 Jahre. Zwischen einer 5-Jahres- und einer 30-Jahres-Prognose steigen selbst die pessimistischen Visionen von 2 % auf ... 80 %. Ende Dezember 2022 gab ein Team chinesischer Universitätsforscher in einer Veröffentlichung bekannt, dass sie in der Lage seien, den RSA-2048-Algorithmus mithilfe einer Quantenmaschine zu entschlüsseln. Doch eine solche öffentliche Kommunikation wirft Fragen auf: Echter technologischer Fortschritt oder eine Warnung an die westlichen Länder? Die Frage bleibt offen.

Aber diese zukünftigen Angriffe können auf den heutigen Daten vorbereitet werden: In ihrer Stellungnahme vom April 2022 erwähnt die französische Behörde ANSSI **den Fall von rückwirkenden Cyberangriffen, die als store now, decrypt later attack** bezeichnet werden. Die Technik, die von anderen auch als *„hack now, decrypt later"*, *„harvest now, decrypt later"*, *„capture now, decrypt later"* usw. bezeichnet wird, besteht darin, schon heute eine sehr große Anzahl verschlüsselter Daten und Kommunikation zu speichern, um sie später, wenn die Quantentechnologie beherrscht wird, wieder zu entschlüsseln. *„Die USA haben diese Art von Angriffen auf sehr langlebige Daten, die ihre Infrastruktur und ihre militärischen Daten betreffen können, bereits beobachtet"*, sagt Arnaud Dufournet. Bevor Sie sich auf die Zukunft konzentrieren: *„Im Bankensektor wird es immer interessant sein, Daten über die Bedingungen und Beträge bestimmter strategischer Transaktionen zu haben. Im Verteidigungssektor sind Informationen über U-Boote jahrzehntelang gültig. Aber auch im Energiesektor, in der Automobilbranche, bei Betriebsgeheimnissen ... Es besteht bereits ein dringender Bedarf an Schutz, da Staaten damit beginnen, Daten zu speichern, um sie später entschlüsseln zu können."* *„Im französischen medizinischen Sektor stellt sich die Frage ebenfalls"*, ergänzt Yvan Vanhullebus, *„da das Gesetz vorsieht, dass eine Gesundheitseinrichtung (öffentlich oder privat) Ihre Krankenakte 20 Jahre lang aufbewahren darf. Auf sichere Weise natürlich."*

„In ihrer Stellungnahme vom April 2022 erwähnt die ANSSI daher den Fall von rückwirkenden Cyberangriffen, die als „store now, decrypt later attack" bezeichnet werden. Die Technik besteht darin, schon heute sehr viele Daten und verschlüsselte Kommunikation aufzuzeichnen, um sie später, manchmal erst Jahre später, zu entschlüsseln, sobald die Quantentechnologie beherrscht wird."

Schließlich könnte auch die Infrastruktur von Krypto-Assets, darunter der viel beachtete Bitcoin, korrumpiert werden, was ihrem Ruf als fälschungssichere Technologie widerspricht. Nach Angaben von Forschern der Universität von Sussex im Vereinigten Königreich könnte eine Quantenmaschine mit 13

Millionen Qubits die Bitcoin-Blockchain innerhalb von nur 24 Stunden hacken. Dann wäre es möglich, Transaktionen umzuleiten und die digitalen Geldbörsen zu leeren. Andere Forschungsarbeiten sind weniger alarmierend und erklären, dass es noch ein oder zwei Jahrzehnte dauern wird, bis diese Leistung erreicht ist. Zum gegenwärtigen Zeitpunkt ist das Hacken des Bitcoin-Netzwerks durch eine Quantenmaschine also noch reine Theorie.

DIE NOTWENDIGE ANPASSUNG VON SICHERHEITSPRODUKTEN

Ein allmählicher Übergang zur Post-Quantum-Kryptografie

Ist die zukünftige Vernichtung der aktuellen Algorithmen zur Datensicherung angesichts des Quantencomputings der Untergang der Verschlüsselung? *„Wenn die gesamte Branche nicht konzertiert reagiert, Ja"*, stellt Yvan Vanhullebus fest. Bevor wir diese Idee einer geplanten Obsoleszenz von Verschlüsselungssystemen nuancieren: *„Es gibt eigentlich keine Alternative, die Algorithmen, Protokolle und Systeme werden sich weiterentwickeln müssen."* Eine Entwicklung, die die Entwicklung mathematischer Algorithmen voraussetzt, die sowohl herkömmlichen als auch zukünftigen Quantenangriffen standhalten können. So wie einige symmetrische Verschlüsselungsalgorithmen: Während der AES128-Algorithmus von einem zukünftigen Quantencomputer als „erledigt" angesehen wird, gilt der AES256-Algorithmus als geschwächt, aber immer noch ziemlich widerstandsfähig. In den USA wird diese Perspektive der nationalen Sicherheit sehr ernst genommen. 2015 präsentierte der kanadische Physiker Michele Mosca das Ergebnis seiner Forschung über die Quantenmechanik und führte gleichzeitig das Theorem ein, das seinen Namen tragen sollte: das Mosca-Theorem. Bei der Suche nach einer Antwort auf die Frage „Wann muss man sich um Quanten sorgen?", theoretisierte er damit, was später zu einem der Gebote der Quantenmechanik werden sollte. Wenn die Summe aus der Zeit, in der verschlüsselte Daten sicher bleiben müssen (X), und der Zeit, die benötigt wird, um die bestehende Infrastruktur mit einer groß angelegten Quantensicherheitslösung umzurüsten (Y), größer ist als die Zeit, die benötigt wird, um einen groß angelegten Quantencomputer oder einen anderen relevanten Fortschritt zu bauen (Z), dann muss man sich Sorgen machen. So hat das amerikanische NIST (*National Institute of Standards and Technologies*) bereits 2016 einen Wettbewerb rund um die Entwicklung von Post-Quanten-Algorithmen ausgeschrieben. Eine Gruppe von vier ersten Gewinnern sowie ihre Algorithmen wurden sechs Jahre später, im Sommer 2022, nach mehreren Runden von Tests und Analysen aller Kandidaten bekannt gegeben. Eine zweite Gruppe von vier weiteren Algorithmen wird derzeit noch untersucht. Parallel dazu erklärte der Direktor für Cybersicherheit der NSA, Rob Joyce, zur gleichen Zeit, dass die Behörde bereits ihre eigenen Algorithmen klassifiziert, die intern entwickelt wurden.

In der Tat **muss nun die gesamte Welt der Cybersicherheit ihren Übergang in eine Post-Quantum-Welt beschleunigen**. Es zeichnen sich mehrere Schwerpunkte ab. Zum einen die Post-Quantum-Kryptografie, bei der neue mathematische Probleme untersucht werden sollen, die den Verschlüsselungsprotokollen zugrunde liegen, um

sie widerstandsfähiger gegen Angriffe zu machen, die durch das Aufkommen großer Quantencomputer möglich werden. Zum anderen die Quantum-Kryptografie, die den physischen Träger der Information verändert, indem sie sich auf neue Quantentechnologien stützt. Die Post-Quantum-Kryptografie ist für das ANSSI „ *der vielversprechendste Weg, um sich gegen die Quantenbedrohung zu schützen*". Dennoch ist die Position der französischen Behörde vorsichtiger als die ihres amerikanischen Pendants NSA, der auf eine schnellstmögliche Einführung von Post-Quantum-Technologien drängt. In einer umfassenden Stellungnahme zur Migration zu Post-Quantum-Kryptografie in einer im April 2022 auf ihrer Website veröffentlichten Stellungnahme rät die französische Behörde der Industrie, schrittweise zu Post-Quantum-Algorithmen überzugehen. Ein hybrider Mechanismus, der somit den Vorteil hat, „*die Berechnungen eines anerkannten Pre-Quantum-Public-Key-Algorithmus und eines zusätzlichen Post-Quantum-Algorithmus*" zu kombinieren und „*sowohl von der starken Zusicherung der Widerstandsfähigkeit des ersten gegen herkömmliche Angreifer als auch von der vermuteten Widerstandsfähigkeit des zweiten gegen Quantenangreifer zu profitieren*". Wie sieht es mit den Anbietern aus, müssen auch sie ihre Verschlüsselungsprotokolle weiterentwickeln, um der Post-Quantum-Verschlüsselung gerecht zu werden? Für Noël Chazotte muss dieser Übergang vollzogen werden, aber eine große Unbekannte bleibt: Welcher Zeitplan soll für die Einführung gelten? Und mit welchen Algorithmen? „*Bei diesem Thema kann man nur in die Richtung des ANSSI gehen: Der Bereich ist noch nicht ausgereift. Und es ist unmöglich, vorherzusagen, wie sich Post-Quantum-Algorithmen in fünf Jahren verhalten werden*", stellt er fest. *Der Algorithmus SIKEwar zum Beispiel lange Zeit ein echtes Versprechen zu diesem Quanten-Thema, bevor seine Anfälligkeit für einen klassischen Angriff im Sommer 2022 von belgischen Forschern aufgedeckt wurde …*"

Quantenschlüsselverteilung (QKD) für präzise Anwendungen

Es gibt Alternativen zur Post-Quantum-Verschlüsselung, die jedoch weniger vielversprechend sind, da sie auf bestimmte Anwendungen beschränkt sind. Dies ist bei der Quantenschlüsselverteilung (*Quantum key distribution – QKD*) der Fall. Dabei handelt es sich um eine Reihe von Protokollen, die es ermöglichen, einen Verschlüsselungsschlüssel zwischen zwei entfernten Gesprächspartnern zu verteilen und gleichzeitig die Sicherheit der Übertragung durch die Gesetze der Quantenphysik und der Informationstheorie zu gewährleisten. Hierbei handelt es sich um eine Familie von Methoden, die auf physischen und nicht wie bei der üblichen Kryptografie auf mathematischen Prinzipien beruhen. Sie ermöglicht es zwei Brieffreunden, „ein gemeinsames Geheimnis" (einen Schlüssel) zu konstruieren, um einen Dialog zu führen. QKD wird in der Regel hervorgehoben, um eine vertrauliche und integre, d. h. von einem Angreifer nicht veränderbare Kommunikation herzustellen. Dazu werden zwei Kanäle benötigt: ein Kanal mit kontrollierten physischen Eigenschaften (eine Glasfaser oder eine direkte Open-Air-Verbindung) ohne Geräte, die mit der transportierten Information interagieren, und eine herkömmliche Netzwerkverbindung.

QKD ist daher völlig abhängig von den physischen Eigenschaften der Kanäle, die sie nutzt, was ihren großflächigen Einsatz „*komplex und kostspielig macht*", urteilt die ANSSI. Darüber hinaus urteilt die französische Agentur, dass die Quantenschlüsselverteilung nicht „ *der natürliche Entwicklungspfad für sichere Kommunikation ist*". Der Grund: Da es keine direkte Linie gibt, die zwei Punkte miteinander verbindet, müssen die Nutzer auf einem aus mehreren Knoten bestehenden Pfad abschnittsweise Schlüssel aushandeln. Dies erfordert jedoch Vertrauen in diese Vermittler. Dies ist „*ein großer Rückschritt im Vergleich zu den derzeitigen Methoden für die Aushandlung von End-to-End-Schlüsseln*", stellt die Behörde fest. Diese Technologie könnte daher nur für Nischenanwendungen genutzt werden.

Von der Theorie zur Industrialisierung

Das Zeitalter des Quantencomputings hat gerade erst begonnen, und die Herausforderungen sind bereits zahlreich. Aktive Beobachtung, Antizipation, Agilität und Anpassung an diese neue Bedrohung sind heute unverzichtbare Kompasse, um zwischen Quanteninformatik und Cybersicherheit zu navigieren. Einerseits ist der technologische Wettlauf zum Quantencomputer komplex und kostspielig. Die Haushaltsinvestitionen in Höhe von mehreren Dutzend Milliarden Euro stellen übrigens ein großes Hindernis dar. Komplex und teuer ist auch der Bedarf an kryptografischen Schutzmaßnahmen gegen Quantenangriffe. Yvan Vanhullebus meint: „*Der theoretische Schritt ist zwar schon getan, aber bis zum Zeitalter der Industrialisierung sind noch einige wirklich große Schritte zu gehen*". Die Standardisierung der ersten Algorithmen war eine davon, aber – so neu sie auch ist – sie braucht noch Zeit, um ihre Stärke und Robustheit wirklich zu bewerten. Parallel dazu müssen auch weitere Standards hinsichtlich ihrer Verwendung in einem hybriden Kontext, wie von der ANSSI empfohlen, erstellt werden. Die Frage stellt sich auch schon heute auf der Ebene der Hardware-Komponenten, die von Natur aus eine echte Trägheit erfahren. „*Das ist ein Thema, das wir bei Stormshield schon früh sehr ernst genommen haben*", erklärt Yvan Vanhullebus. *Für unsere Stormshield Network Security Firewalls zum Beispiel sind wir bereits dabei, die neuesten Infineon TPM zu integrieren, die einzige TPM-Komponente auf dem Markt, die Post-Quantum-Schutz bietet*."

Es ist wichtig, dass alle Akteure im Bereich der Cybersicherheit bereits jetzt Maßnahmen ergreifen, um das Zeitalter des Quantencomputings und das Zeitalter der Post-Quanten-Krypto zu antizipieren. **Das Ziel? Nicht Opfer, sondern Akteure dieser wichtigen technologischen Entwicklung zu sein**. In diesem Kontext sucht Europa seinen Platz.