

Quantenkryptographie als Thema für den Physikunterricht

- Vorstellung einer Masterarbeit -

Cordula Reisch*, Torsten Franz*

* Technische Universität Braunschweig, IFdN, Abt. Physik & Physikdidaktik
c.reisch@tu-bs.de, torsten.franz@tu-braunschweig.de

Kurzfassung

Quantenkryptographie ist ein modernes Forschungsgebiet der Physik, welches einen motivierenden Kontext für die Grundkonzepte der Quantenphysik bieten kann. Im Rahmen einer Masterarbeit wurde eine Unterrichtssequenz zur Quantenkryptographie mit Photonen erstellt und an einem Physikkurs der 11. Jahrgangsstufe getestet. Wir stellen die Unterrichtsmaterialien sowie die Ergebnisse von Interviews und Fragebögen vor.

1. Einleitung

Quantenphysik ist ein typisches Thema der gymnasialen Oberstufe und in vielen Bundesländern curricular verankert. Sie ist oft das einzige Thema der modernen Physik und gilt häufig als besonders unanschaulich und lebensfern. Ein möglicher Weg, um diesen beiden Kritikpunkten zu begegnen, könnte eine stärkere Fokussierung auf Themen der Quanteninformation sein (vgl. [1] und Referenzen darin).

In der hier vorgestellten Arbeit haben wir eine Unterrichtssequenz zur Quantenkryptographie erstellt, welche als Einstieg in das Thema Quantenphysik dienen soll. Das Ziel hierbei ist einerseits durch die Wahl eines aktuellen und technologisch (zumindest perspektivisch) anwendbaren Kontextes eine höhere Motivation für das Thema zu erzeugen und andererseits durch die Diskussion eines konkreten Beispiels die Anschaulichkeit zu erhöhen. Hierzu wurde ein einfaches Analogie-Experiment mit polarisierten Lichtstrahlen eingesetzt, um daraus Rückschlüsse auf das Verhalten von Einzelphotonen zu ziehen.

Die Unterrichtssequenz wurde in einer 11ten Klasse eines niedersächsischen Gymnasiums durchgeführt. Zur Evaluation wurde zunächst ein Fragebogen für alle Schülerinnen und Schüler und zusätzlich Interviews mit einigen Schülerinnen und Schülern durchgeführt. Es nahmen 19 Schülerinnen und Schüler an der Einheit teil, wobei das Thema Quantenphysik in der Schule noch nicht vorher behandelt wurde.

Wir stellen im Folgenden zunächst kurz die Unterrichtssequenz vor und diskutieren dann schwerpunktmäßig die Evaluation und ihre Ergebnisse. Die Sequenz wurde im Rahmen einer Masterarbeit entwickelt [2]. Eine detaillierte Beschreibung des Vorgehens und des physikalischen Hintergrunds findet sich in [3], die verwendeten Arbeitsblätter, Materialien und Lösungen finden sich unter [4].

2. Beschreibung der Unterrichtssequenz

Die Unterrichtssequenz wurde über zwei Doppelstunden durchgeführt und gliedert sich in drei Abschnitte: In der ersten Stunde wurde das Prinzip der klassi-

schen Kryptographie am Beispiel von unterschiedlichen Verschlüsselungsverfahren erklärt. Das Ziel hierbei war, neben einem motivierenden Einstieg, die Betonung der Wichtigkeit des sicheren Schlüssels für die Kryptographie. Den Schülerinnen und Schülern sollte am Ende der Stunde klar sein, dass mit Hilfe einer One-Time-Pad Verschlüsselung abhörsichere Kommunikation möglich ist, hierzu aber zunächst ein sicherer Schlüssel verteilt werden muss, was mit den Mitteln der klassischen Physik nicht möglich ist.

In der zweiten Hälfte der ersten Doppelstunde wurde das Konzept von Einzelphotonen (als unteilbare Zustände des Lichts) eingeführt und die Möglichkeit besprochen, auch Einzelphotonen zu polarisieren. Die Polarisation von Lichtstrahlen war in der Klasse bereits bekannt, daher wurde daran nur kurz erinnert. Um das Verhalten von polarisiertem Licht beim Durchgang durch Polfilter zu demonstrieren, wurde mit einem einfachen Aufbau (siehe Abb. 1) das Verhalten bei parallelen, orthogonalen und um $+45^\circ$ verdreht eingestellten Polarisatoren gezeigt. Dann wurde der Übergang vom Demonstrationsexperiment (Intensitätsmessung) zum äquivalenten Experiment mit Einzelphotonen gemacht und die Wahrscheinlichkeit für eine Detektion als Ergebnis einer Messung definiert. In der zweiten Doppelstunde wurde schließlich das BB84-Kryptographie-Protokoll [5] erklärt und die Sicherheit der Quantenkryptographie besprochen.

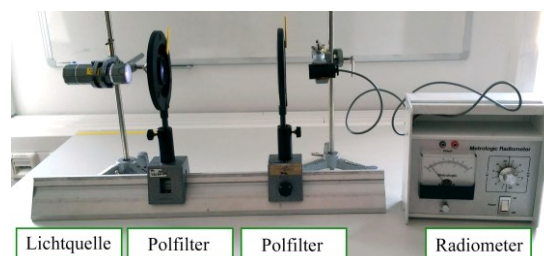


Abb.1: Aufbau des Experiments

Konzeptionell wurde sich hierbei an den didaktischen Modellen von Müller [6] sowie Müller und Küblbeck [7] orientiert und besonders die Quanteneigenschaften „statistisches Verhalten“ und „Keine Messung

ohne Störung“ betont (vgl. hierzu auch Kapitel A1 in [8]). Am Ende der Einheit sollten die Schülerinnen und Schüler in der Lage sein, die Sicherheit der Quantenkryptographie mit der Unmöglichkeit von störungsfreien Messungen begründen zu können.

3. Auswertung der Fragebögen

Der erste Teil der Evaluation war ein zweigeteilter Fragebogen. Im ersten Teil wurden motivationale Aspekte mit 13 Items auf einer vierstufigen Likert-Skala abgefragt. Hierbei waren die ersten sechs Items aus dem Kurztest intrinsische Motivation nach Wilde [9] übernommen. Die Ergebnisse sind in Tabelle 1 dargestellt.

Hieraus lässt sich schließen, dass der Unterricht tendenziell als motivierend und interessant wahrgenommen wurde, wobei jedoch keine Vergleichsuntersuchung zu anderen Themen des Unterrichts durchgeführt wurde. Interessant ist das Antwortverhalten bei Frage 7: Hier gaben 9 Schülerinnen und Schüler an, sich schon einmal mit dem Thema Kryptographie beschäftigt haben (z.T. im schulischen Wahlkurs Informatik) während 9 Schülerinnen und Schüler die Angaben „eher nicht“ oder „nicht“ gewählt haben. Dieses inhaltliche Ungleichgewicht des Vorwissens werden wir auch in den weiteren Untersuchungen noch sehen. Bei dieser Frage ergab sich auch ein signifikant unterschiedliches Antwortverhalten von Schülern im Vergleich mit den Schülerinnen, da alle Antworten der Kategorie „Stimmt genau“ von Schülern gegeben wurden. Etwas überraschend ist weiterhin das Antwortverhalten bei Frage 8, wonach 11 Schülerinnen und Schüler das Thema Kryptographie als unbedeutend für ihren jeweiligen Alltag angeben. Wir werden im Ausblick Möglichkeiten diskutieren, dem zu begegnen.

Der zweite Teil des Fragebogens bestand aus drei offenen Fragen: „Nenne Sie drei Dinge, die Ihnen an der Unterrichtseinheit gefallen haben“, „Nennen Sie drei Dinge, die Ihnen an der Unterrichtseinheit nicht so gut gefallen haben“ und „Welche Wünsche und Verbesserungsvorschläge haben Sie“. Auf die erste Frage wurden 56 Einzelantworten gegeben, auf die zweite Frage 31 Einzelantworten und auf die dritte Frage noch 17 Einzelantworten.

Wir fassen nun die Ergebnisse der ersten beiden Fragen zusammen, wobei wir hier nur Antwortkategorien erwähnen, denen mindestens 5 Einzelantworten zugeordnet werden konnten. Ausschließlich positiv wurden die Experimente und die Aktualität des Themas, überwiegend positiv wurden die ausführlichen Aufgabenblätter sowie die Verständlichkeit bewertet. Ambivalent war das Urteil über das langsame Tempo des Vorgehens. Überwiegend negativ wurden die recht langen Diskussionen bewertet. Die Ergebnisse finden sich mit Beispielimens in Tabelle 2.

Die Antworten auf die dritte Frage sind weniger eindeutig; einzig die Wünsche „mehr Lenkung in der Diskussion“ und „Schüler [und Schülerinnen] mehr

experimentieren lassen“ wurden jeweils zweimal genannt.

4. Auswertung der Interviews

Nach Ablauf der beiden Doppelstunden wurden mit vier Schülerinnen und Schülern leitfadengestützte Interviews im Umfang von jeweils etwa 20 Minuten geführt. Sie fanden drei Tage nach der zweiten Doppelstunde statt und wurden zweimal als Einzelinterview und einmal als Doppelinterview durchgeführt.

Die Interviews waren inhaltlich in einen motivationalen Teil zu Beginn und einen fach-inhaltlichen Teil gegliedert, wobei sich der fach-inhaltliche Teil am Ablauf der beiden Doppelstunden orientierte.

Bezüglich des Interesses ergab sich ein Unterschied hinsichtlich des Vorwissens, was die klassische Kryptographie angeht. Diejenigen Schülerinnen und Schüler, die das Thema bereits im Informatikunterricht behandelt hatten, empfanden den Teil im Unterricht als zu lang und gaben starkes Interesse an der Quantenkryptographie an. Diejenigen, die noch keine Erfahrung mit klassischer Kryptographie hatten, gaben den Aspekt des Unterrichts als besonders interessant an, wobei speziell das „Selbermachen“ beim Entschlüsseln als motivierend benannt wurde.

Inhaltlich konnte die klassische Kryptographie gut wiedergegeben werden. So wurden in allen Interviews die Caesar-Chiffre und die One-Time-Pad-Verschlüsselung erwähnt.

Bei Fragen zur Vorstellung über Licht und Photonen zeigt sich, dass in allen Interviews die Vorstellung von Photonen als kleine, unteilbare Lichtteilchen vorherrschte. Weiter ist ein deutlicher Einfluss von Vorinformation erkennbar: In einem Interview wurde explizit angegeben, dass der Schüler oder die Schülerin schon mal etwas davon gehört habe, dass Quantenobjekte „Welle und Teilchen zugleich“ seien. In einem weiteren Interview wurde erwähnt, dass sich Elektronen „gleichzeitig links und rechts herum drehen“ können und dass ein Quantenobjekt erst durch eine Messung einen Zustand annehme. All dies wurde nicht im Unterricht angesprochen.

Bezüglich der Sicherheit von Quantenkryptographie wurde in allen Interviews erwähnt, dass sich der Angreifer hinsichtlich des übertragenen Schlüssels nicht sicher sein kann und raten muss. In zwei Interviews wurde die perfekte Zufälligkeit des Schlüssels als besonderes Kriterium erwähnt und in einem Interview weiterhin die Möglichkeit benannt, einen Angreifer in der Quantenkryptographie zu entdecken.

5. Ergebnisse / Diskussion

Unsere Untersuchung der Unterrichtssequenz hat gezeigt, dass die Einheit grundsätzlich als Einstiegsunterricht geeignet ist. Sowohl bei den Erhebungen zur Motivation, als auch beim punktuell erfassten Fachwissen konnte ein positiver Status nach Ende der Einheit festgestellt werden.

Die Untersuchung hat aber auch Schwachpunkte des Ansatzes gezeigt: Da die Schülerinnen und Schüler sehr unterschiedliches Vorwissen in klassischer Kryptographie mitbrachten, war ein angemessenes Tempo für alle Schülerinnen und Schüler schwer zu finden. Hier könnte ein Anreicherungsangebot für Schülerinnen und Schülern mit großen Vorwissen hilfreich sein, damit sich diese Schülerinnen und Schüler beim Einstieg nicht langweilen. Wir haben in den Materialien [4] ein zusätzliches Aufgabenblatt zur asymmetrischen Kryptographie und zum RSA-Algorithmus hinzugefügt, welches möglicherweise einen Ansatz bieten kann (auch wenn es noch kein bearbeitbares Aufgabenblatt ist).

Gerade in den Interviews wurde deutlich, dass die Vorstellungen der Schülerinnen und Schüler nach der Unterrichtssequenz in einigen Aspekten (z.B. Unteilbarkeit des Einzelphotonenzustandes) der Zielvorstellung entsprachen, jedoch daneben noch weitere Vorstellungen vorlagen, welche nicht Teil des Unterrichts waren und bei denen die Anwendung auf das betrachtete Beispiel nicht ohne Weiteres möglich scheint. Der Umgang mit solchen (Fehl-) Vorstellungen, die z.T. durch die Diskussion der Quantenphysik in den populären Medien beeinflusst zu sein scheint, ist aber eine größere Herausforderung, welche erst in Rahmen einer längeren Unterrichtseinheit (mehr als zwei Doppelstunden) systematisch angegangen werden kann. Es wäre spannend zu sehen, wie die Schülerinnen und Schüler ihre Vorstellungen konkret mit dem gegebenen Experiment in Verbindung bringen. Dies könnte ein Ansatz für weitere Untersuchungen sein.

Durch die Fragebögen haben wir gesehen, dass die Schülerinnen und Schüler das Thema Kryptographie nicht als Teil ihres Alltags begreifen. Um eine Verbindung herzustellen, könnte zu Beginn der ersten Unterrichtsstunde die Bedeutung der Verschlüsselung für unsere heutige Informationsgesellschaft sowie Nutzen und Risiken diskutiert werden. Hier können im Unterricht Zeitungsmeldungen (beispielsweise zur Bedeutung von Kryptographie beim Onlinebanking oder den sozialen Netzen, oder der Gefahr durch Verschlüsselung im Dark Net) als Impulse verwendet werden.

Die Schülerinnen und Schüler wünschten sich bei den Experimenten mehr Beteiligung. Auch hier könnte man eine Variante der Unterrichtssequenz verwenden, bei der Experimente in Gruppen durchgeführt werden. Die Materialien sollten an vielen Schulen vorhanden sein, wobei das verwendete Radiometer auch durch ein Luxmeter oder den Helligkeitssensor eines Fotohandys oder Tablets ersetzt werden kann. Die linearen Polarisatoren können durch kommerzielle 3D-Brillen realisiert werden, die in der Kinotechnik zum Einsatz kommen.

6. Zusammenfassung

Wir haben in einer 11ten Klasse eine Unterrichtssequenz zur Quantenkryptographie als Einstieg in die

Quantenphysik durchgeführt und evaluiert. Die Evaluation ergab insgesamt ein hohes Interesse und bei den nachfolgenden Interviews einen guten Umgang mit den vermittelten Inhalten. Es ergaben sich aber auch deutliche Unterschiede bezüglich des Vorwissens, was die Quantenphysik und die Informatik angeht.

7. Literatur

- [1] Themenheft Quanteninformation (2016), PdN-Physik in der Schule, 1/65
- [2] Reisch, C. (2015): Quantenkryptographie als Thema für den Physikunterricht. Masterarbeit TU Braunschweig
- [3] Reisch, C.; Franz, T. (2016): Quantenkryptographie. In: PdN - Physik in der Schule, 1/65, S.11-16
- [4] <http://www.tu-braunschweig.de/ifdn/physik/mitarbeiter/torstenfranz/veroeffentlichungen/material/> (Stand 05/2016)
- [5] Bennett, C.H.; Brassard, G. (1984): Quantum Cryptography: Public key distribution and coin tossing. In: Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, S. 175
- [6] Müller, R.; Strahl, A.; Dammaschke, T.: milq – Quantenphysik an der Schule; Online-Lehrgang, <http://www.milq-physik.de/> (Stand 05/2016)
- [7] Müller, R.; Küblbeck: Die Wesenszüge der Quantenphysik (2002), Praxis-Schriftreihe, Aulis Verlag Deubner Köln
- [8] Franz, T. QuantH - Kurssystem zu den Grundlagen der Quantenphysik und der Quanteninformation, <http://www.quantH-physik.de> (Stand 05/2016)
- [9] Wilde, M.; Bätz, K.; Kovaleva, A.; Urhahne, D. (2009): Überprüfung einer Kurzskaala intrinsischer Motivation (KIM). In: Zeitschrift für Didaktik der Naturwissenschaften 15, 31-45

Nr.	Text	Stimmt genau	Stimmt eher	Stimmt kaum	Stimmt nicht
1	Die Unterrichtseinheit Quantenkryptographie hat mir Spaß gemacht.	6	11	2	0
2	Ich fand das Thema Quantenkryptographie sehr interessant.	11	7	1	0
3	Das Bearbeiten des Temas war unterhaltsam.	2	14	2	0
4	Mit meiner Leistung in der Unterrichtseinheit bin ich zufrieden.	5	8	5	0
5	Bei Aufgaben zur Kryptographie stelle ich mich geschickt an.	2	14	2	0
6	Ich glaube, ich war bei der Mitarbeit in der Unterrichtseinheit sehr gut.	3	8	5	1
7	Ich habe mich zuvor schon einmal mit dem Thema Kryptographie beschäftigt.	9	1	6	3
8	Das Thema Kryptographie kommt in meinem Alltag vor.	1	3	4	11
9	Die Unterrichtseinheit hat mein Interesse am Thema geweckt.	0	9	8	1
10	Ich empfand den Stoff der Unterrichtseinheit als zu einfach.	1	7	11	0
11	Ich freue mich darauf, nächstes Halbjahr mehr über Quantenphysik zu erfahren.	10	6	2	1
12	Ich glaube, ich habe bei der Unterrichtseinheit viel gelernt.	7	8	3	0
13	Ich würde gerne erneut ein aktuelles Forschungsgebiet im Unterricht behandeln.	10	8	1	0

Tabelle 1: Ergebnisse des ersten Teils des Fragebogens. Die Medianwerte sind rot fett hervorgehoben.

	Kategorie	Beispielitem	Positive Erwähnung	Negative Erwähnung
↑	Experiment	„Anschaulichkeit durch den Versuch“	11	0
	Thema	„interessantes Thema“	8	0
↗	Aufgabenblätter	„gute Arbeitsblätter“ (positiv); „zu viele Zettel“ (negativ)	9	3
	Verständlichkeit	„gut verständlich“ (positiv); „deutlicher Herausarbeiten der Thesen“ (negativ)	9	5
→	Langsames Vorgehen	„langsames Erarbeiten des Stoffes“ (positiv); „viele Wiederholungen“ (negativ)	6	5
↘	Viele Diskussionen	„Wir durften viel selber diskutieren“ (positiv); „im Kreis laufende Diskussionen“ (negativ)	3	7

Tabelle 2: Ergebnisse des zweiten Teils des Fragebogens. Die Pfeile deuten an, ob Kategorien ausschließlich positiv ↑, überwiegend positiv ↗, ambivalent → oder überwiegend negativ ↘ bewertet wurden.