Dr. Christian Wolny

Dramatisierte Quantenkryptographie

Karl Svozil

Zusammenfassung

Moderiert durch Spielleiter und informierte Mitspieler werden Besucher darin angehalten, sich selbst als Elementarquant zu erleben und sich im Rahmen eines kryptographischen Protokolls wie ein solches zu verhalten.

Antonin Artaud gewidmet,
dem Autor von *Le théâtre et son double* [1].

1. Hintergrund

Quantenkryptographie ist ein relativ junges, außerordentlich aktives Forschungsgebiet der Quantenphysik, dessen Haupteigenschaft die Verwendung einzelner Teilchen zur verschlüsselten Informationsübertragung ist. Ziel ist das Erstellen und Vergrößern von geheimen gleichen Zufallszahlen zwischen zwei räumlich getrennten Agenten. Dies wird durch Elementarquanten, zum Beispiel einzelne Photonen ermöglicht, welche in einem Quantenkanal übermittelt werden.

Die Geschichte der Quantenkryptographie begann bereits um 1970 mit einem Manuskript von Wiesner [2] und mit dem BB84-Protokoll von Bennett&Brassard [3, 4, 5, 6, 7]. Die bisherigen experimentellen Realisierungen sind zahlreich; sie reichen, um nur einige Beispiele anzuführen und ohne Anspruch auf Vollständigkeit, von den ersten Experimenten im IBM Yorktown Heights Laboratory [6] im Jahre 1989 über Signalübertragungen zwischen den Ufern des Genfer Sees 1993 [7], dem bestehenden, seit 2003 kontinuierlich von der DARPA betriebenen Netz in der Boston Metropolitan Area [8] bis zur publikumswirksamen Banküberweisung durch optische Lichtwellenleiter in Abwasserkanälen in Wien unter Beisein von Lokalpolitikern und Bankenvertretern [9].

Quantenkryptographie als Teil von Quanteninformationstechnologien stellt ein wesentliches Bindeglied zwischen theoretischer Grundlagenforschung und experimentellen, technologischen und eventuell industriellen Anwendungen dar. Sie benutzt den neuesten Stand der Quantenphysik, um in zunehmendem Maße komplexe physikalische und mathematisch-algorithmische Probleme zu lösen.

In der Öffentlichkeit besteht großes Interesse an Quantenphysik und Quantenkryptographie; doch werden die verwendeten Protokolle kaum je öffentlich im Detail vorgestellt. Für den Außenstehenden erscheinen diese Gebiete in einer Art „mystischen Schleier" [10] gehüllt, der nur schwer zu durchdringen ist. Mit dem Versuch, Quantenkryptographie erlebbar zu machen, wird den Akteuren Einblick in diese Protokolle gegeben.

2. Vermittlungsansatz

2.1 Prinzipien

Um Quantenkryptographie erlebbar zu machen, soll sie dramatisiert werden. Die quantenkryptographischen Protokolle werden in Form eines Schauspiels umgesetzt, wobei Schauspieler und Moderator unter aktiver Einbeziehung des Publikums die „Quantenbühne" nachempfinden. Besucher werden eingeladen, bei der Umsetzung der quantenkryptographischen Protokolle mitzuspielen. Die Moderation sollte nach Möglichkeit von einem Kabarettisten oder einem Physik- bzw. Deutschlehrer durchgeführt werden. Denkbar wäre auch eine Zusammenarbeit mit schulischen Schauspielgruppen.

Zugute kommt hierbei die prinzipielle Analogie der Dramaturgie zum Experiment, durchaus im surrealen Sinn [1]: auch Einzelteilchen-Quantenexperimente laufen nicht total deterministisch ab; sie werden unter anderem von Zufallsereignissen bestimmt und von einem Grundrauschen „geprägt"; genauso wie das zu erwartende moderierte Chaos der öffentlich aufgeführten quantenkryptographischen Protokolle.

Mögliche „Störaktionen" einzelner Teilnehmer sind dabei sogar erwünscht. Dabei sollte der Spaß an der Sache, die Gelassenheit und der Versuch, sich in ein Elementarquant hineinzudenken und sich als solches zu fühlen und erleben, im Vordergrund stehen; ganz im Sinne des meditativen Zen Koans „Mu". Dann wird es vielleicht sogar gelingen, sich wie die Schrödinger'sche Katze [11] zu fühlen, oder auch wie in ein Teilchen, welches durch zwei räumlich getrennte Spalten gleichzeitig schlüpft. Aber diese Form von körperlicher Entäußerung ist weder notwendig noch besonders wichtig für die vorgeschlagene Dramatisierung quantenkryptographischer Protokolle.

In der Folge geht es um die Realisierung des schon erwähnten, von Bennett&Brassard vorgeschlagenen BB84-Protokolls. Die Ausführung ist inspiriert von Wright's verallgemeinertem Urnenmodell [12], und der äquivalenten [13] Automatenlogik [14]. Unsere gesamte empirische Welterkenntnis beruht letztlich auf dem Eintreten von elementaren (binären) Ereignissen, wie etwa die Reaktionen, die Quanten in Teilchendetektoren hervorrufen. Auf diesen syntaktisch elementaren Vorfällen basiert die Semantik, das heißt ihre Deutung und Bedeutung mit Begriffen und Theorien. Man sollte des-

halb nicht so unbescheiden sein, nachfolgende einfache syntaktische Regeln als bloße Kochrezepte abzutun. Denn auch die Quantenmechanik ist nichts anderes als ein sophistisches Regelwerk mit semantischem Überbau, welches sich gelegentlich sogar populistischer Floskeln wie etwa „Beamen" bedient. Was das untenstehende Protokoll allerdings entscheidend von der Quantenmechanik unterscheidet, ist die Verwendung von verborgenen Parametern; dh. die prinzipiell durchgängige Bestimmtheit aller möglichen Messgrößen.

2.2 Ausführung

Ziel ist die Erstellung einer geheimen zufälligen Zahlenfolge, die nur zwei Agenten, im Folgenden „Anna" und „Alex" genannt, kennen. Erforderlich sind dafür folgende Utensilien:

(1) jeweils zwei rot und zwei grün getönte Brillen in voller Farbsättigung (Komplementärfarben);

(2) eine Urne oder Kübel;

(3) Eine größere Anzahl von Schokobällchen in der Urne. Die Bällchen, zum Beispiel Mozartkugeln oder Ähnliches, sollten idealerweise mit Stanniolpapier umwickelt sein, welches auf schwarzem Untergrund jeweils ein rotes und ein grünes Symbol – entweder „0" oder „1" – aufgedruckt hat. Es gibt vier Balltypen entsprechend allen Kombinationen von zweifarbigen Symbolen. Diese sind in Tabelle 1 aufgelistet. Alle vier Balltypen kommen gleich häufig vor.

Tabelle 1: Beschriftung der Schokoballtypen auf schwarzem Untergrund.

Balltyp	rotes Symbol	grünes Symbol
Typ 1	rote 0	grüne 0
Typ 2	rote 0	grüne 1
Typ 3	rote 1	grüne 0
Typ 4	rote 1	grüne 1

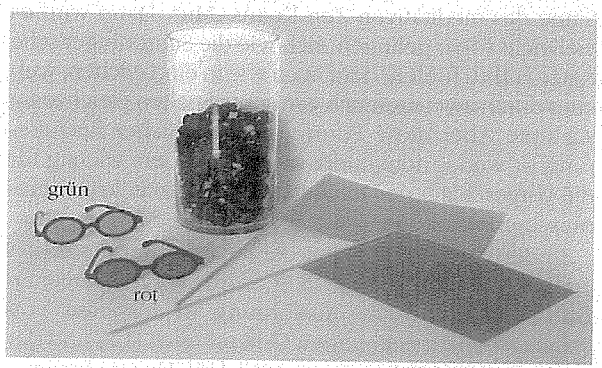
(4) zwei rote und zwei grüne Fähnchen;

(5) zwei Tafeln samt Kreiden (alternativ zwei geheime Schulhefte);

(6) zwei Münzen.

Abbildung 1 zeigt die zur Dramatisierung des BB84-Protokolls erforderlichen Utensilien.

Abb. 1: Utensilien zur Dramatisierung des BB84-Protokolls



Folgende handelnde Personen treten auf und ab:

(1) Ein Moderator, der das Geschehen kommentiert und die Einhaltung des untenstehenden Protokolls mehr oder weniger (nach Belieben) sicherstellt. Diesem ist große Freiheit gegeben, etwa auch kryptographische Angriffe zu inszenieren;

(2) Darsteller, welche das Protokoll kennen und neue Besucher als Mitspieler-Quantenen bzw. in der Rolle von Anna und Alex einweisen;

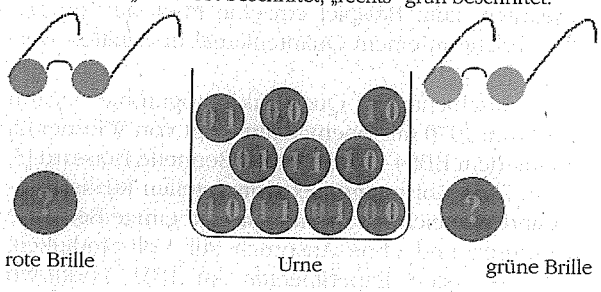
(3) Besucher in großer Zahl, auch „Mitspieler-Quanten" genannt, welche die Schokobällchen übertragen und hernach verspeisen.

Schokobällchen mit roten Symbolen 0 und 1 entsprechen zum Beispiel in der Quantenoptik horizontal und vertikal polarisierten Photonen. Schokobällchen mit grünen Symbolen 0 und 1 entsprechen zum Beispiel in der Quantenoptik links- oder rechts zirkular polarisierten Photonen; oder alternativ zum Beispiel auch linear polarisierten Photonen, deren Polarisationsrichtungen und um einen Winkel von 45° ($\pi/4$) aus der Horizontalen und Vertikalen gedreht wurden.

Das Protokoll läuft nun folgendermaßen ab:

(1) Zunächst wirft Anna eine Münze und wählt damit eine von zwei Brillen aus: entweder eine grün getönte Brille für „Kopf", oder eine rot getönte Brille für „Zahl". Sie setzt sich diese Brille auf und zieht nun zufällig einen Ball aus der Urne. Anna kann nur das Symbol in der Farbe ihrer Brille lesen. (Durch die subtraktive Farbmischung erscheint das andere Symbol in der Komplementärfarbe schwarz). Die Situation ist in der Abbildung 2 wiedergegeben. Anna schreibt die Symbole aller Karten, die sie losschickt entweder auf eine Tafel oder in ihr Heft. (Sollte Anna Anstalten machen, die Brille abzunehmen oder das Bällchen mit der anderen Brille zu betrachten, hat das Mitspieler-Quant Anweisung, es sofort aufzuessen.)

Abb. 2: Wright's verallgemeinertes Urnenmodell. Kugeln in der Urne „links" rot beschriftet, „rechts" grün beschriftet.



(2) Anna überreicht den gezogenen Ball einem Mitspieler-Quant, welches ihn zum Empfänger Alex trägt. (Hierbei gehen einige Mitspieler-Quanten bzw. deren Bälle verloren und kommen, aus welchen Gründen auch immer, nie an. Es gibt ja besondere Naschkatzen, die nicht abwarten können und ihr Schokobällchen sofort auswickeln und essen!)

(3) Bevor Alex das Bällchen vom Mitspieler-Quant in Empfang nimmt bzw. mustert, wirft er nun ebenfalls eine Münze und wählt damit ebenfalls eine von zwei Brillen aus: entweder die grün getönte Brille für „Kopf", oder die rot getönte Brille für „Zahl". Er setzt sich diese Brille auf und betrachtet damit die von den Mitspieler-Quanten erhaltenen Kugeln. Alex wird ebenfalls nur ein Symbol am Schokobällchen lesen können, weil das andere Symbol ja in der Komplementärfarbe aufgedruckt ist und ihm schwarz erscheint. Er macht nun ebenfalls eine Eintragung aller Symbole, die er gelesen hat. (Sollte Alex Anstalten machen, die Brille abzunehmen oder das Bällchen mit der anderen Brille zu betrachten, hat das Mitspieler-Quant Anweisung, es sofort aufzuessen!)

(4) In der Folge teilt Alex nun Anna mit seinem Fähnchen mit, ob er überhaupt eine Karte erhalten hat, und welche Brille er beim Empfang aufhatte. Er teilt ihr aber nicht das von ihm abgelesene Symbol selbst mit.

(5) Im Gegenzug teilt Anna mit ihrem Fähnchen Alex mit, welche Brille sie aufhatte. Sie teilt ihm aber nicht das von ihr abgelesene Symbol selbst mit.

(6) Alex und Anna behalten nur diejenigen Symbole, deren Bälle sie beide erhielten, und die sie mit der gleichen Brillenart (gleiche Fähnchen) betrachtet haben.

(7) Die so ausgewählten Symbole stellen eine zufällige Reihe von Nullen und Einsen dar, welche identisch für Anna und Alex ist. Diesen zufälligen Schlüssel kann man für viele kryprographische Anwendungen verwenden; z. B. als „One-Time-Pad" wie die TANs beim Online-Banking. (Einige Symbole werden von Anna und Alex direkt verglichen, um zu sehen, ob sich etwa ein Angreifer eingeschlichen hat.)

Das Mitspieler-Quant kann sein Schokobällchen entweder selbst aufessen oder es weiterverschenken.

2.3 Alternative Variante

Nachfolgend wird noch eine alternative Protokollvariante vorgestellt, die eine einfachere Umsetzung ermöglicht. Sollten die für das obige Protokoll notwendigen Requisiten verfügbar gemacht werden können (z. B. färbige Brillen), kann erforderlichenfalls auf dieses zurückgegriffen werden. Jedoch ist vom dramaturgisches Standpunkt betrachtet die erste Variante zu bevorzugen.

Die alternative Variante entspricht eher den quantenmechanischen Zuständen (falls man klassische Analogien überhaupt als sinnvoll erachtet); insbesonders die Vermeidung der gleichzeitigen Bestimmtheit zweier „komplementärer" Observablen, in diesem Fall rot und grün. Hierbei wird zuerst nur einer der beiden Kontexte definiert (entweder rot oder grün), und danach zufällig ein von dieser Wahl unabhängiger Kontext gemessen. Stimmen die beiden Kontexte nicht überein (rot-grün oder grün-rot), erfolgt eine Kontextübersetzung [15] durch Münzwurf und es gibt keine Korrelation der beiden Symbole; stimmen sie überein (rot-rot oder grün-grün), erhält man identische Ergebnisse, das heißt identische Symbole.

Statt der Bällchen kommen jeweils zwei einheitlich gefärbte Schokofiguren der Form „0" und „1" in den Komplementärfarben rot und grün zum Einsatz (siehe Tabelle 2).

Tabelle 2: Färbung der Schokofiguren.

Balltyp	rotes Symbol	grünes Symbol
Typ 1	–	grüne 0
Typ 2	–	grüne 1
Typ 3	rote 0	–
Typ 4	rote 1	–

Die Schokofiguren befinden sich zuerst in einer Urne. Die Häufigkeit der Figurentypen soll wieder gleich sein. Dieses Protokoll kommt ohne getönte Brillen aus.

(1) Zuerst wählt Anna aus der Urne eine zufällige Figur, macht sich eine Aufzeichnung darüber (Wert 0 oder 1 und Farbe) und übergibt die Figur in der Folge dem Mitspieler-Quant.

(2) Das Mitspieler-Quant trägt die Figur zu Alex.

(3) Alex wirft eine Münze und wählt damit eine von zwei Farben aus: „Kopf" steht für grün, „Zahl" für rot. Ist die Farbe von Alex und die Farbe der von Anna gewählten und vom Mitspieler-Quant präsentierten Figur identisch (rot-rot oder grün-grün), dann gilt das Symbol der Figur. Sind die Farben unterschiedlich (rot-grün oder grün-rot), dann nimmt Alex das Resultat seines Münzwurfes und ordnet „Kopf" dem Symbol 0 zu, sowie „Zahl" dem Symbol 1. (Alex kann, wenn er will, für diese Zuordnung auch noch einmal extra würfeln.) In jedem Fall macht auch Alex sich eine Aufzeichnung des von ihm ermittelten Symbols.

(4–7) Die weiteren Schritte sind identisch mit dem ersten Protokoll in Abschnitt 2.2.

2.4 Angriffe und Abhören der Quantenverschlüsselung

Es ist erlaubt, verschiedenste friedliche „Angriffe" auf das Protokoll durchzuführen, die ein Mithören der verschlüsselten Nachrichten ermöglichen. Dabei ist wichtig, dass beim ersten Protokolltyp jeder potentielle Angreifer selbst ebenfalls eine getönte Brille trägt. Weiters ist es niemandem gestattet, auch nicht den Mitspieler-Quanten, sich weitere Schokobällchen oder Figuren aus der Urne zu holen, die identisch mit dem ürsprünglichen sind.

Der erfolgversprechendste Abhöransatz ist die auch im GSM-Netz häufig zur Anwendung kommende „man-in-the-middle"-Attacke, bei der es dem Angreifer gelingt, gegenüber Anna wie Alex aufzutreten und gegenüber Alex wie Anna. Effektiv werden dabei zwei quantenkryptographische Protokolle in Serie geschaltet oder voneinander komplett unabhängig abgewickelt. Gegen diesen Angriff ist die Quantenkryprographie, entgegen den oft gehörten Versicherungen ihrer absoluten Abhörsicherheit, die gewissermaßen von den Naturgesetzen garantiert wird, nicht immun.

3. Unterschiede zu „richtigen" Quanten

Die Frage: „Welcher Unterschied existiert nun eigentlich zur ‚wahren' Quantenkryptographie?" ist wohl der kostbare Preis der Veranstaltung. Nach unserer Erfahrung wird sie durchaus von Mitarbeitern und Publikum gestellt. Im Unterricht wird man sie unter Umständen selbst stellen müssen.

Der eigentliche Unterschied liegt in zumindest zwei Ursachen begründet: den Schokobällchen, welche keine genuine Quanten darstellen, und die Brillen, die uns die Weltsicht trüben. Denn die Brillen können von uns abgenommen werden, und wir sehen dann beide Symbole in den Komplementärfarben rot und grün gleichzeitig. Dies ist quantenmechanisch nicht möglich; hier gibt es keine gleichzeitige Sicht auf komplementäre Messgrößen. Dies zeichnet ja gerade Komplementarität aus, und das kann anhand der Schokobällchen schön demonstriert werden: dass man sich entscheiden muss, welche von zwei oder mehreren komplementären Größen man misst. Nach so einem solchen Messprozess sind die anderen Messgrößen unbestimmt.

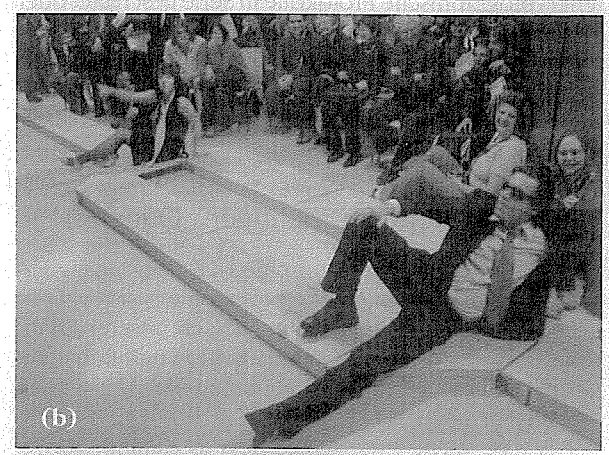
Die Analogie von Schokobällchen und Quanten ist noch wesentlich problematischer als es der erste Anschein vermuten lässt. Denn in der Quantenwelt gewis-

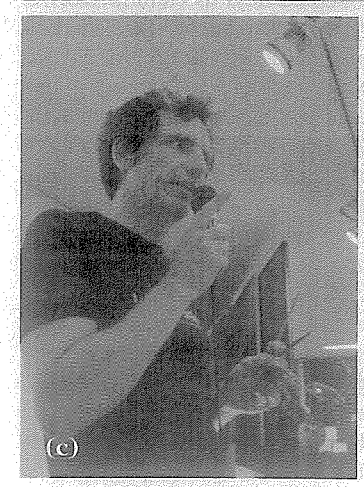
se dürften Quanten eine durchgehende und konsistente Färbung wie bei den Schokobällchen gar nicht zulassen. Dies ist der Inhalt eines sehr schönen und tiefen Theorems von Kochen & Specker [16]: heuristisch gesprochen ist es unmöglich, eine hypothetische Gesamtheit an Beobachtungen nicht aus Teilbeobachtungen zusammen zu setzen.

4. Erfahrungen

Die vorgestellten Protokolle wurden das erste Mal im Rahmen der Langen Nacht der Forschung am 1. Oktober 2005 an der Technischen Universität Wien durchgeführt. Dabei herrschte ein unerwartet reges Interesse; sowohl an den Schokobällchen, als am Mitspielen, und vor Allem an Theorie und Praxis der Quantenkryptographie! Abbildung 3 zeigt einige Bilder von dieser Aufführung. Ich kann nur alle Leser ermuntern, es einmal selbst zu versuchen – mit einem dankbaren Publikum und einem lebendigen Andenken an den Unterricht kann gerechnet werden!

Abbildung 3: Szenen der ersten Aufführung





Literatur

[1] Antonin Artaud. *Le théâtre et son double.* Gallimard, Paris, 1938.

[2] Stephen Wiesner. Conjugate coding. *Sigact News,* 15: 78–88, 1983. Manuskript geschrieben um 1970 [6].

[3] Charles H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. Quantum cryptography, or unforgable subway tokens. In *Advances in Cryptography: Proceedings of Crypto '82,* pages 78–82, New York, 1982. Plenum Press.

[4] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India,* pages 175–179. IEEE Computer Society Press, 1984.

[5] Artur Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters,* 67: 661–663, 1991.

[6] Charles H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology,* 5: 3–28, 1992.

[7] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Review of Modern Physics,* 74: 145–195, 2002.

[8] Chip Elliott, Alexander Colvin, David Pearson, Oleksiy Pikalo, John Schlafer, and Henry Yeh. Current status of the DARPA quantum network. 2005.

[9] A. Poppe, A. Fedrizzi, T. Loruenser, O. Maurhardt, R. Ursin, H. R. Boehm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger. Practical quantum key distribution with polarization-entangled photons. *Optics Express,* 12: 3865–3871, 2004.

[10] Anton Zeilinger. *Einsteins Schleier.* Beck, München, 2003.

[11] Erwin Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften,* 23: 807–812, 823–828, 844–849, 1935.

[12] Ron Wright. Generalized urn models. *Foundations of Physics,* 20: 881–903, 1990.

[13] Karl Svozil. Logical equivalence between generalized urn models and finite automata. *International Journal of Theoretical Physics,* page in print, 2005.

[14] Karl Svozil. *Quantum Logic.* Springer, Singapore, 1998.

[15] Karl Svozil. Quantum information via state partitions and the context translation principle. *Journal of Modern Optics,* 51: 811–819, 2004.

[16] Simon Kochen und Ernst Specker, The Problem of Hidden Variables in Quantum Mechanics, *Journal of Mathematics and Mechanics,* 17: 59–87, 1967.

Anschrift des Verfassers:
Institut für Theoretische Physik, Technische Universität Wien,
Wiedner Hauptstraße 8–10/136, 1040 Wien,
http://tph.tuwien.ac.at/~svozil, svozil@tuwien.ac.at