Staging quantum cryptography with chocolate balls[a)]

Karl Svozil[b)]
Institut für Theoretische Physik, University of Technology Vienna, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

(Received 17 October 2005; accepted 21 April 2006)

Moderated by a director, laypeople and students assume the role of quanta and enact a quantum cryptographic protocol. The performance is based on a generalized urn model capable of reproducing complementarity even for classical chocolate balls. © *2006 American Association of Physics Teachers.*

[DOI: 10.1119/1.2205879]

This paper is dedicated to Antonin Artaud, author of *Le théâtre et son double*.[1]

I. BACKGROUND

Quantum cryptography is a relatively recent and very active field of research. Its main characteristic is the use of individual particles for encrypted information transmission. Its objective is to encrypt messages or to create and enlarge a set of secret equal random numbers between two spatially separated agents by means of elementary particles, such as single photons, that are transmitted through a quantum channel.

The history of quantum cryptography dates back to around 1970 to the manuscript by Wiesner[2] and a protocol by Bennett and Brassard[3–7] in 1984, henceforth called BB84. Since then, experimental prototyping has advanced rapidly. Without going into too much detail and just to name a few examples, the work ranges from the first experiments carried out at the IBM Yorktown Heights Laboratory by Bennett and co-workers in 1989,[6] to signal transmissions across Lake Geneva in 1993,[7] and the network in the Boston area which has been sponsored by DARPA since 2003.[8] In a much publicized spectacular demonstration, a quantum cryptographic-aided bank transfer took place via optical fibers installed in the sewers of Vienna.[9]

Quantum cryptography forms an important link between quantum theory and experimental technology, and possibly even industrial applications. The public is greatly interested in quantum physics and quantum cryptography, but the protocols used are rarely made available to the layperson or student in any detail. For an outsider, these subjects seem to be shrouded in a kind of "mystic veil" and are very difficult to understand.

In what follows, a play will be proposed which closely follows quantum cryptographic protocols. It involves a moderator, actors, and possibly spectators, and requires a couple of properly colored chocolate balls (the chocolate is not essential, but pleasant). The coloring of the chocolate balls follows a simple but effective generalized urn model introduced by Wright[10–12] to mimic complementarity. A generalized urn model is characterized by an ensemble of balls with a black background color. Printed on these balls are color symbols from a symbolic alphabet. A particular ball type is associated with a unique combination of monocolored (no mixture of wavelength) symbols printed on the black ball background. Every ball contains just one single symbol per color.

Assume further, some monospectral filters or eyeglasses that are perfect and that totally absorb light of all other colors but a particular one. In this way, every color can be associated with a particular eyeglass and vice versa.

When one looks at a particular ball through such an eyeglass, the only operationally recognizable symbol will be the one with the particular color that is transmitted through the eyeglass. All other colors are absorbed, and the symbol on the ball will appear black and therefore cannot be differentiated from the black background. Hence, the ball appears to carry a different message or symbol depending on the eyeglass through which it is viewed. We will present an explicit example featuring complementarity, which is similar in many ways to quantum complementarity.

The difference between the chocolate (black) balls and quanta is the possibility of viewing all of the different symbols on the chocolate balls by taking off the eyeglasses. Quantum mechanics does not provide us with such a possibility. On the contrary, there are strong arguments suggesting that the assumption of a simultaneous physical existence[13] of such complementary observables yields a complete contradiction,[14–16] a result that has recently been experimentally confirmed.[17]

The differences between the quasi-classical and the quantum cases should be made explicit. The protocols used with the quasi-classical chocolate ball model appear very similar to the quantum mechanical ones. However, we should not conclude that in the quantum domain there merely exist some constraints on the measurements (such as the monocolored glasses) that prevent us from perceiving the "real" picture. In the quantum domain, the simultaneous imprinting of different symbols in different colors is impossible, in general. This impossibility can be a very good starting point for a better understanding of quantum systems and their differences with classical systems.

II. PRINCIPLES OF CONDUCT

To make quantum cryptography a real-life experience, we have turned the quantum world into a drama in which actors and a moderator present a quantum cryptographic protocol on stage. The audience is actively involved in the presentation. If possible, the event should be moderated by a well-known comedian or by a physics teacher.

The entire play is analogous to a surreal experiment: Single quanta are not completely predictable. Their behavior is determined by random events, and marked by the "noise" that would accompany the public presentation of the quantum cryptographic protocols. Therefore, the interference of individual participants is even encouraged and not a deficiency of the performance.

Table I. Schema for imprinting of the chocolate balls.

Ball type	Red	Green
1	0	0
2	0	1
3	1	0
4	1	1

Throughout the performance, everybody should have fun, relax, and try to feel and act like an elementary particle in the spirit of the meditative Zen koan. The participants might try to feel like Schrödinger's cat[18] or like a particle simultaneously passing through two spatially separated slits. We might contemplate how conscious minds could experience a coherent quantum superposition between two states of consciousness. However, this kind of sophistication is neither necessary nor important for dramatizing quantum cryptographic protocols.

Our entire empirical knowledge of the world is based on the occurrence of elementary (binary) events, such as the reactions caused by quanta in particle detectors yielding a click. Therefore, the following simple syntactic rules should not be dismissed as mere recipes, for even quantum mechanics can be considered to be a sophisticated set of laws with a possibly superfluous[19] semantic superstructure.

III. INSTRUCTIONS FOR STAGING THE PERFORMANCE

Our objective is to generate a secret sequence of random numbers known only by two agents, Alice and Bob. To do so, the following utensils will be required:

1. Two sets each of fully saturated eyeglasses in red and green (complementary colors).
2. An urn or bucket.
3. A large number of foil-wrapped chocolate balls (called Mozartkugeln in Austria) or similar balls, each with a black background imprinted with one red and one green symbol (either 0 or 1) to be placed inside the urn. The symbols can, for instance be prepared as color stickers shaped in different geometries (e.g., circles and stars or squares). There are four types of balls, which are listed in Table I. There are an equal number of each type in the urn.
4. Small red and green flags, two of each.
5. Two blackboards and chalk (or two secret notebooks).
6. Two coins.

The following actors are involved:

1. A moderator who makes comments and ensures that the participants more or less adhere to the protocol as described below. The moderator has many liberties and may even choose to stage cryptographic attacks.
2. Alice and Bob, two spatially separated parties.
3. Ideally, but not necessarily, some actors who know the protocol and introduce new visitors to the roles of Alice, Bob, and the quanta.
4. A large number of people assuming the roles of the quanta. They are in charge of transmitting the chocolates and may eat them in the course of events or afterward.

In the performance, chocolates marked with the symbols 0 and 1 in red correspond to horizontally (↔) and vertically (↕) polarized photons in quantum optics, respectively. Chocolates marked with the symbols 0 and 1 in green correspond to left and right circularly polarized photons, or alternatively to linearly polarized photons with polarization directions (⤢) and (⤡) rotated by 45° from the horizontal and the vertical, respectively.

In the basic quantum key distribution protocol mimicked here, Alice sends Bob a random sequence of polarized photons in four states belonging to two different conjugate bases. (These four states correspond to the four different kinds of balls; the two bases correspond to the two complementary colors.) In the second phase, Bob chooses randomly and independently of Alice which one of the two different conjugate bases he wishes to use to perform his photon measurements. (This choice will correspond to Bob's choice of colored eyeglass.) Bob then performs the measurements and records both the results (corresponding to the symbols read through the colored eyeglass) as well as his measurement basis (corresponding to the color of the eyeglass) for each photon. Bob then announces publicly the bases (colors) chosen, but not the outcome of his measurements. Alice compares these bases (colors) to the ones she used in sending out the photons (balls). They then publicly agree to use the matching bases (colors), thereby discarding all events in which their bases (colors) are different, or in which Bob has not received any photon at all. In a final step, they form a (random) sequence by taking the succession of all of these outcomes, coded in a binary alphabet.

In more detail, the protocol is as follows:

1. Alice flips a coin to chose one of the two pairs of glasses; heads for the green glasses, tails for the red ones. She puts them on and randomly draws a chocolate from the urn. She can only read the symbol in the color of her glasses. She writes the symbol she can read and the color used, either on the blackboard or in her notebook. Should she take off her glasses or look at the symbols with the other pair, the player carrying the chocolate ball is required to eat it at once.
2. After writing down the symbol, Alice hands the chocolate to the quantum, who carries it to the recipient Bob. During this process, the chocolate could become lost and never reach its destination (those with a sweet tooth might, for example, not be able to wait and eat their chocolate immediately).
3. Before Bob can take the chocolate and look at it, he needs to flip a coin to choose a pair of glasses. He puts on the glasses and takes a look at the chocolate ball he has just received. He, too, will only be able to read one of the symbols, because the other one is imprinted in the complementary color and appears black to him. Then, he makes a note of the symbol he has read and the color used. As before, should he take off his glasses or look at the symbols with the other glasses, the quantum is required to eat the chocolate at once.
4. After the legal transmission has taken place, the quantum may eat the chocolate ball just transferred from Alice to Bob, or give it away.
5. Now Bob uses one of the two flags (red or green) to tell Alice whether he has received anything at all and what color his glasses are. He does not communicate the symbol itself.

6. At the same time, Alice uses one of her flags to inform Bob of the color of her glasses. She also does not tell Bob the symbol she identified.
7. Alice and Bob only register the symbol on a blackboard or on a note if they both received the corresponding chocolate, and if the color of their glasses (that is, their flags) matched. Otherwise, they dismiss the entry.
8. The entire process (1–7) is repeated several times.

As a result, Alice and Bob obtain an identical random sequence of the symbols 0 and 1 representing identical outcomes. This random sequence can be interpreted as a "random key" that could be used in a cryptographic application. A more amusing application is to let Alice communicate to Bob secretly whether (1) or not (0) she would consider giving him her cell phone number. For this task, only a single bit of the sequence they have created is required. Alice forms the sum $s=i\oplus j=i+j \bmod 2$ of her decision i and the secret bit j, and cries it out loudly over to Bob. Bob can decode Alice's message to plain text by simply forming the sum $s\oplus t=i$ of Alice's encrypted message s and the secret bit $t=j$ shared with Alice, for $j\oplus t=j\oplus j=0$. This task is a romantic and easily communicable way of employing one-time pads generated by quantum cryptography.

Alice and Bob compare some of the symbols directly to make sure that there has been no attack by an eavesdropper. Indeed, if the eavesdropper Eve is bound to one color and cannot perceive both symbols imprinted on the balls simultaneously, then she will sometimes choose the wrong color, which does not match Alice's and Bob's. If Eve digests the chocolate after observing it (and does not merely retransmit it), she can only guess the symbol in the other color with a 50:50 chance. Thus, the new ball she has to send to Bob will carry the wrong symbol in one-half of the cases, when her color does not match Alice's and Bob's color. Hence, if Alice and Bob compare some of their symbols, they could realize that Eve is listening.

IV. ALTERNATIVE PROTOCOLS

There exist numerous possible variants of the dramatization of the BB84 protocol. A great simplification would be the total abandonment of the black background of the chocolate balls as well as the colored eyeglasses. In this case, both Alice and Bob simply decide by themselves which colored eyeglasses to take and record the symbols in the color chosen.

In the following, we will present yet another BB84-type protocol within the context of the translation principle.[20] First, Alice (the sender) defines one of two possible contexts or colors; in this case, either red or green. Then, the receiver Bob chooses another color, which is independent of Alice's choice. If the two colors do not match, a color (or context)[20] translation is carried out by flipping a coin. In this case, there is no correlation between the two symbols.

In this protocol, we use sets of two chocolate figures shaped like 0 and 1, and uniformly colored in red and green, as shown in Table II. An equal amount of each type of figure is placed inside an urn. No colored glasses are necessary to carry out this protocol.

The protocol is as follows:

Table II. Color and geometry of the four chocolate figures.

Ball type	Red	Green
1	—	0
2	—	1
3	0	—
4	1	—

1. First, Alice randomly draws one figure from the urn and makes a note of its value (0 or 1) and its color. Then she gives the figure to one of the spectators carrying the figures.
2. The quantum carries the figure to Bob.
3. Bob flips a coin and chooses one of two colors.
   (a) If the color corresponds to that of the figure chosen by Alice and presented by the quantum, the symbol of the figure counts and Bob makes a note of the symbol and its color.
   (b) If it does not correspond, Bob takes the result of the coin he has just flipped and assigns heads to 0 and tails to 1. This results in a randomization of the outcome, just as in quantum mechanics. If he wishes, he may flip the coin again and use the new result instead; just to emphasize the distinction between the random choice related to the type of measurement and the random outcome.

In any case Bob writes down the resulting symbol and the color.

4. The remaining steps correspond to the previous protocol.

With this protocol Alice and Bob, by keeping the symbols in the matching colors, arrive at two identical random sequences on their sides. If chocolate balls are not readily available, the advantage of this procedure over the protocol involving black chocolate balls with red and green symbols imprinted on them is that here only two arbitrary but different geometric shapes of chocolate pieces in two different colors are required.

V. FURTHER DRAMATURGICAL ASPECTS, ATTACKS, AND REALIZATION

It is possible to scramble the protocol in its simplest form and thus the encryption by drawing two or more chocolate balls, with or without identical symbols on them, from the urn at once; or by breaking the time order of events. This would correspond to technological problems related to implementations of quantum cryptography.

It is allowed to eavesdrop on the encrypted messages. For the first protocol, every potential eavesdropper needs to wear colored glasses. Note that no one (not even the quanta) may take additional chocolates or chocolate figures from the urn, which are identical to the one originally drawn by Alice. In a sense, this rule implements the no-cloning theorem, which states that it is not possible to copy an arbitrary quantum if it is in a coherent superposition of the two classical states.

The most promising eavesdropping strategy is the man-in-the-middle attack, which is often used in mobile phone networks. The attacker manages to impersonate Bob when communicating with Alice and vice versa. What basically happens is that two different quantum cryptographic proto-

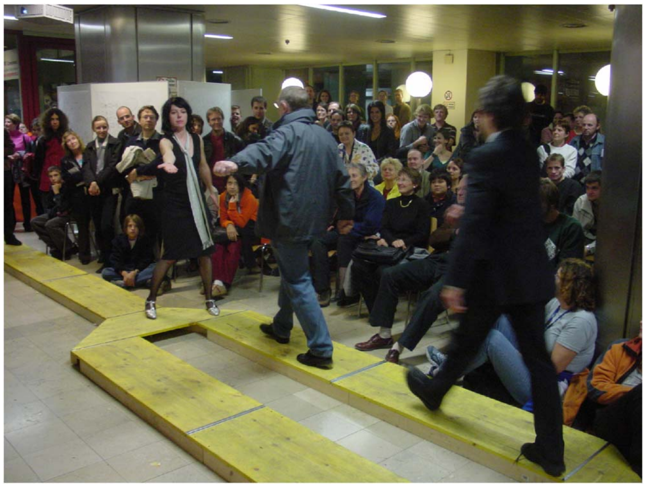

Fig. 1. A player carrying a chocolate ball across the walkway. Some “agents” try to steal the chocolate ball.

cols are connected in series, or carried out independently from each other. Quantum cryptography is not immune to this kind of attack.

The first performance of the quantum drama we have sketched took place in Vienna at the University of Technology as a part of “Lange Nacht der Forschung” (long night of science). Experience showed that a considerable fraction of the audience obtained some understanding of the protocol; in particular, the players acting as Alice and Bob. The photograph in Fig. 1 depicts a player trying to carry a chocolate ball across a walkway. Most of the audience got the feeling that quantum cryptography is not so cryptic after all.

For students of physics, the most important questions are those related to the differences and similarities between chocolate balls and quanta. It should be stated quite clearly from the beginning that, although the quasi-classical protocols resemble the quantum cryptographic ones, there are fundamental differences with regard to the quantum physical properties and observables: It is not just sufficient to assume that quantum properties are hidden by operational inaccessibility, such as colored eyeglasses blocking the recognition of symbols painted in the complementary color. In quantum physics, the Bell-type, Kochen-Specker, and Greenberger-Horne-Zeilinger theorems[21] lead to the conclusion that certain observables do not have a defined value prior to their measurement. The quasi-classical analogies discussed here serve as a good introduction to the quantum cryptographic protocols, and are also a good motivation and starting point for considerations of quantum complementarity and value indefiniteness.

ACKNOWLEDGEMENTS

The idea for this paper was born over a coffee conversation with Günther Krenn. The first public performance was sponsored by Lange Nacht der Forschung, ⟨www.langenachtderforschung.at⟩. The chocolate balls were donated by Manner ⟨www.manner.com⟩, and the black foil covering the balls was donated by Constantia Packaging ⟨www.constantia-packaging.com⟩. Thanks go to Karin Peter and the public relation office of the TU Vienna for providing the infrastructure, to the Impro Theater for the stage performance, and to Martin Puntigam for moderating part of the performances. A second performance took place at Auckland University’s Centre for Discrete Mathematics and Theoretical Computer Science.

[a] The author reserves the copyright for all public performances. Performance licenses are granted for educational institutions and other not-for-profit performances for free; these institutions are kindly asked to send a small note about the performance to the author.

[b] Electronic address: svozil@tuwien.ac.at; http://tph.tuwien.ac.at/~svozil

[1] A. Artaud, *Le théâtre et Don Double* (Gallimard, Paris, 1938).

[2] S. Wiesner, “Conjugate coding,” SIGACT News **15**, 78–88 (1983). Manuscript written *circa* 1970. (Ref. 6).

[3] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, “Quantum cryptography, or unforgable subway tokens,” in *Advances in Cryptography: Proceedings of Crypto ’82* (Plenum Press, New York, 1982), pp. 78–82.

[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* (IEEE Computer Society Press, 1984), pp. 175–179.

[5] A. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett. **67**, 661–663 (1991).

[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” J. Cryptology **5**, 3–28 (1992).

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,”Rev. Mod. Phys. **74**, 145–195 (2002).

[8] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, “Current status of the DARPA quantum network,” quant-ph/0503058.

[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,” Opt. Express **12**, 3865–3871 (2004) or quant-ph/0404115.

[10] R. Wright, “Generalized urn models,” Found. Phys. **20**, 881–903 (1990).

[11] R. Wright, “The state of the pentagon. A nonclassical example,” in *Mathematical Foundations of Quantum Theory*, edited by A. R. Marlow (Academic Press, New York, 1978), pp. 255–274.

[12] K. Svozil, “Logical equivalence between generalized urn models and finite automata,” Int. J. Theor. Phys. **44**, 745–754 (2005) or quant-ph/0209136.

[13] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?,” Phys. Rev. **47**, 777–780 (1935).

[14] S. Kochen and E. P. Specker, “The problem of hidden variables in quantum mechanics,” J. Math. Mech. **17**, 59–87 (1967).

[15] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Going beyond Bell’s theorem,” in *Bell’s Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic Publishers, Dordrecht, 1989), pp. 73–76.

[16] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, “Bell’s theorem without inequalities,” Am. J. Phys. **58**, 1131–1143 (1990).

[17] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, “Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement,” Nature (London) **403**, 515–519 (2000).

[18] E. Schrödinger, “Die gegenwärtige Situation in der Quantenmechanik,” Naturwiss. **23**, 807–812, 823–828, 844–849 (1935); URL ⟨http://wwwthep.physik.uni-mainz.de/~matschul/rot/schroedinger.pdf⟩.

[19] C. A. Fuchs and A. Peres, “Quantum theory needs no interpretation,” Phys. Today **53**, 70–71 (2000); [Further discussions of the article can be found in Phys. Today **53**, 11–14 (2000)].

[20] K. Svozil, “Quantum information via state partitions and the context translation principle,” J. Mod. Opt. **51**, 811–819 (2004) or quant-ph/0308110.

[21] N. D. Mermin, “Hidden variables and the two theorems of John Bell,” Rev. Mod. Phys. **65**, 803–815 (1993).

[22] E. Specker, *Selecta* (Birkhäuser Verlag, Basel, 1990).

[23] J. D. Trimmer, “The present situation in quantum mechanics: A translation of Schrödinger’s ’cat paradox’,” Proc. Am. Philos. Soc. **124**, 323–338 (1980).

[24] J. A. Wheeler and W. H. Zurek, *Quantum Theory and Measurement* (Princeton University Press, Princeton, N.J., 1983).