Staging quantum cryptography with chocolate balls[*]

Karl Svozil[†]

Institut für Theoretische Physik, University of Technology Vienna,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

Moderated by a director, laymen and students are encouraged to 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.

Dedicated to Antonin Artaud,
author of *Le théâtre et son double* [1].

I. BACKGROUND

Quantum cryptography is a relatively recent and extremely active field of research within quantum physics. Its main characteristic is the use of (at least ideally) 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, which 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 & Brassard in 1984 [3–7] 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 very first experiments carried out in 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 Metropolitan 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 in the presence of some local politicians and bank representatives [9].

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

In what follows, we shall use 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 black background color. Printed on these balls are some color symbols from a symbolic alphabet. The colors are elements of a set of colors. A particular ball type is associated with a unique combination of mono-spectrally (no mixture of wavelength) colored symbols printed on the black ball background. Every ball contains just one single symbol per color.

Assume further some mono-spectral filters or eyeglasses which are "perfect" by totally absorbing light of all other colors but a particular single one. In that way, every color can be associated with a particular eyeglass and vice versa.

When a spectator looks at a particular ball through such an eyeglass, the only operationally recognizable symbol will be the one in the particular color which is transmitted through the eyeglass. All other colors are absorbed, and the symbols printed in them 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 color at which it is viewed. We will present an explicit example featuring complementarity, in very similar ways as quantum complementarity.

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

Therefore, the differences between the quasi-classical and the quantum cases should be clearly spelled out. The protocols and procedures referring to the quasi-classical chocolate ball model appear very similar to the quantum mechanical ones. However, one should not be lead to the conclusion that in the quantum domain there merely exist some constraints on the measurments (such as the mono-colored glasses) which prevent us from perceiving the "real, full" picture. – In the quantum domain, the simultaneous imprinting of different symbols in different colors is impossible in the general case! Indeed, this can be a very good starting point for a better understanding of the quantum, and its differences with classical

---

II. PRINCIPLES OF CONDUCT

In order to make it a real-life experience, we have aimed at dramatizing quantum cryptography. The quantum world is turned into a kind of drama, in which actors and a moderator present a quantum cryptographic protocol on stage. The audience is actively involved and invited to participate in the dramatic presentation. If at all possible, the event should be moderated by a well-known comedian, or by a physics teacher.

The entire process is principally analogous to an experiment in a slightly surreal sense: just like humans, single quanta are never completely predictable. Among other things, they are in fact determined by random events, and marked by a certain "noise" similar to the chaos that will certainly accompany the public presentation of the quantum cryptographic protocols. Therefore, the interference of individual participants is even encouraged and not a deficiency of the model.

Throughout the performance, everybody should have fun, relax, and try to feel and act like an elementary particle – rather in the spirit of the meditative Zen koan "Mu." The participants might manage to feel like Schrödinger's cat [18], or like a particle simultaneously passing through two spatially separated slits. In idle times, one may even contemplate how conscious minds could experience a coherent quantum superposition between two states of consciousness. However, this kind of sophistication is neither necessary, nor particularly 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 either a "click" or none. Therefore, the following simple syntactic rules should not be dismissed as mere cooking recipes, for quantum mechanics itself can actually be applied merely as a sophisticated set of laws with a possibly superfluous [19] semantic superstructure.

III. INSTRUCTIONS FOR STAGING THE PROTOCOL

Our objective is to generate a secret sequence of random numbers only known by two agents called Alice and Bob. In order to do so, the following utensils depicted in Figure 1 will be required:

(1) Two sets each of fully saturated glasses in red and green (complementary colors)

(2) An urn or bucket

(3) A large number of foil-wrapped chocolate balls (in Austria called "Mozartkugeln") or similar – each with a black background, imprinted with one red and one green symbol (either 0 or 1) – to be placed inside the urn. According to all possible combinations, there are four types altogether, which can be found in Table I.

FIG. 1: Utensils required for staging the BB84 protocoll.

ball type	red	green
1	0	0
2	0	1
3	1	0
4	1	1

TABLE I: Schema of imprinting of the chocolate balls.

There needs to be 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 acting persons 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 necessary are 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 afterwards.

In our model, chocolates marked with the symbols 0 and 1 in red, correspond to what in quantum optics correspond to horizontally ($\leftrightarrow$) and vertically ($\updownarrow$) polarized photons, respectively. Accordingly, chocolates marked with the symbols 0
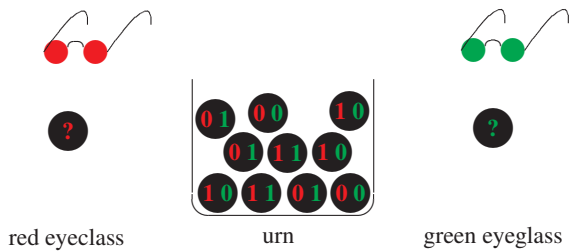
FIG. 2: Wright's generalized urn model put to practical cryptographic use.

and 1 in green, correspond to left ($\circlearrowleft$) and right ($\circlearrowright$) circularly polarized photons, or alternatively to linearly polarized photons with polarization directions ($\nearrow$) and ($\searrow$) rotated by 45 ($\pi/4$) from the horizontal and the vertical, respectively.

The protocol is to be carried out as follows:

(1) Alice flips a coin in order to chose one of two pairs of glasses: heads is for the green glasses, tails for the red ones. She puts them on and randomly draws one chocolate from the urn. She can only read the symbol in the color of her glasses (due to subtractive color the other symbol in the complementary color appears black and cannot be differentiated from the black background). This situation is illustrated in Figure 2. She writes the symbol she could read, as well as the color used, either on the blackboard or into her notebook. Should she attempt to take off her glasses or look at the symbols with the other pair, the player in the role of the quantum is required to eat the chocolate at once.

(2) After writing down the symbol, Alice hands the chocolate to the quantum, who in turn carries it to the recipient Bob. During this process, it could, however, get lost and for some reason 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 may take the chocolate and look at it, he, too, needs to flip a coin in order to choose one pair of glasses. Again, heads is for the green, and tails for the red ones. He puts them on and takes a look at the chocolate ball he has just received. He, too, will only be able to read one of the symbols, as 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, as well as of the color used. As before, should he attempt to take off his glasses or look at the symbols with the other pair, the quantum is required to eat the chocolate at once.

After the legal transmission has taken place, the "quantum" may eat the chocolate ball just transfered from Alice to Bob, or give it away, anyway.

(4) 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, however, communicate the symbol itself.

At the same time, Alice uses one of her flags to inform Bob of the color of her glasses. Again, she does not tell Bob the symbol she identified.

(5) Alice and Bob only keep the symbol if they both received the corresponding chocolate, and if the color of their glasses (i.e. their flags) matched. Otherwise, they dismiss the entry.

The whole process (1-5) is then repeated several times.

As a result, Alice and Bob obtain an identical random sequence of the symbols 0 and 1. The random key can be used in many cryptographic applications, for instance as one-time pad (like TANs in online banking). A more amusing application is to let Alice communicate to Bob secretly whether (1) or not (0) she would consider giving him her mobile phone number. For this task merely a single bit of the sequence they have created is required. Alice forms the sum $i \oplus j = i + j \bmod 2$ of her decision and the secret bit and cries it out loudly over to Bob. Bob can decode Alice's message to plain text by simply forming the sum $s \oplus t$ of Alice's encrypted message s and the secret bit $t = j$ shared with Alice, for $j \oplus t = 0$. Indeed, this seems to be a very romantic and easily communicable way of employing one-time pads generated by quantum cryptography. (And seems not too far away from the phantasies of its original inventors ;-)

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, not matching Alice's and Bob's. If Eve digests the chocolate after observing it (and 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 half the cases when her color does not match Alice's and Bob's color. Thus, if Alice and Bob compare some of their symbols, they could realize that Eve ist listening.

IV. ALTERNATIVE PROTOCOL VERSIONS

There exist numerous possible variants of the dramatization of the BB84 protocol. A great simplification can 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 color to take, and record the symbols in the color chosen.

In the following, we will present yet another BB84-type protocol with the context translation principle [20]. First of all, we define one of two possible "contexts" or colors; in this case either red or green. Then we randomly measure another color, which is independent of this choice. If the two colors do not match (red-green or green-red), a "color (or context [20]) translation" is carried out by flipping a coin. In this case, there is no correlation between the two symbols. If, however, the

ball type	red	green
1	—	0
2	—	1
3	0	—
4	1	—

TABLE II: Coloring and geometry of the four chocolate figures.

two colors match (red-red or green-green), the results, i.e. the symbols, are identical.

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 figures is placed inside an urn. No colored glasses are necessary to carry out this protocol.

The protocol is to be carried out as follows:

(1) First of all, Alice randomly draws one figure from the urn and makes a note of its value (0 or 1) and of its color. Then she gives the figure to one of the quanta.

(2) The quantum carries the figure to Bob.

(3) Bob flips a coin and thus chooses one of two colors. Heads is for green, tails for red. If the color corresponds to that of the figure drawn by Alice and presented by the quantum (red figure–red draw or greenfigure–green draw), the symbol of the figure counts. If it does not correspond (red figure–green draw or green figure–red draw), Bob takes the result of the coin he has just flipped and assigns heads to 0 and tails to 1. If he wants to, he may flip it again and use the new result instead. In any case Bob writes down the resulting symbol.

(4-5) The rest corresponds to the protocol presented previously.

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.

It is allowed to carry out peaceful attacks in order to to eavesdrop on the encrypted messages. In the case of the first protocol, every potential attacker needs to wear colored glasses herself. 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 stating 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 so-called man-in-the-middle attack, which is often used in GSM networks. The attacker manages to impersonate Bob when communicating with Alice and vice versa. What basically happens is that two different quantum cryptographic protocols 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 sketched above took place in Vienna at the University of Technology as a parallel part of an event called "Lange Nacht der Forschung" ("long night of science"). Figure 3a) depicts the "quantum channel," a "catwalk" constructed from yellow painted form liners lifted on the sides with planed wood planks, through which the individual "quanta" had to pass from Alice to Bob. In the middle of the catwalk, the path forked into two passes, which joined again – some allusion to quantum interference. The photographs in Figure 3b)-f) depict some stages of the performance.

Experience showed that a considerable fraction of the audience obtained some understanding of the protocol; in particular the players acting as Alice and Bob. Most people from the audience got the feeling that quantum cryptography is not so cryptic after all, if they are capable of performing the protocol and even have fun experiencing it.

For the student of physics probably 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, whereas the quasiclassical protocols resemble the quantum cryptographic ones very much, 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" or "vailed" by operational inaccessibility, such as colored eyeglasses blocking the recognition of symbols painted in the complementary color. In quantum physics, by Belltype, Kochen-Specker, and Greenberger-Horne-Zeilinger theorems [21], one is lead to the conclusion that certain observables do not have a defined value prior to their measurement. Hence, the quasi-classical analogies discussed here may not only serve as a good introduction into the quantum cryptographic protocols, but may also be a good motivation and starting point for considerations about quantum complementarity and value-indefiniteness, as well as for the type of experience presented by single-quantum experiments.

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

[2] S. Wiesner, "Conjugate coding," Sigact News **15**, 78–88 (1983). Manuscript written *circa* 1970 [6, Ref. 27].

[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*, pp. 78–82 (Plenum Press, New York, 1982).

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

[5] A. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters **67**, 661–663 (1991).

[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," Journal of Cryptology **5**, 3–28 (1992).

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Review of Modern Physics **74**, 145–195 (2002). URL `http://dx.doi.org/10.1103/RevModPhys.74.145`.

[8] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA Quantum Network," (2005). 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," Optics Express **12**, 3865–3871 (2004). quant-ph/0404115, URL `http://www.opticsinfobase.org/ViewMedia.cfm?id=80796\&seq=0`.

[10] R. Wright, "Generalized urn models," Foundations of Physics **20**, 881–903 (1990).

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

[12] K. Svozil, "Logical equivalence between generalized urn models and finite automata," International Journal of Theoretical Physics **44**, 745–754 (2005). quant-ph/0209136, URL `http://dx.doi.org/10.1007/s10773-005-7052-0`.

[13] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Physical Review **47**, 777–780 (1935). URL `http://dx.doi.org/10.1103/PhysRev.47.777`.

[14] S. Kochen and E. P. Specker, "The Problem of Hidden Variables in Quantum Mechanics," Journal of Mathematics and Mechanics **17**(1), 59–87 (1967). Reprinted in [22, pp. 235–263].

[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*, M. Kafatos, ed., pp. 73–76 (Kluwer Academic Publishers, Dordrecht, 1989).

[16] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, "Bell's theorem without inequalities," American Journal of Physics **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 **403**, 515–519 (2000).

[18] E. Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik," Naturwissenschaften **23**, 807–812, 823–828, 844–849 (1935). English translation in [23] and [24, pp. 152-167], URL `http://wwwthep.physik.uni-mainz.de/~matschul/rot/schroedinger%.pdf`.

[19] C. A. Fuchs and A. Peres, "Quantum theory needs no 'Interpretationt'," Physics Today **53**(4), 70–71 (2000). Further discussions of and reactions to the article can be found in the September issue of Physics Today, *53*, 11-14 (2000), URL `http://www.aip.org/web2/aiphome/pt/vol-53/iss-9/p11.htmlandhttp://www.aip.org/web2/aiphome/pt/vol-53/iss-9/p14.html`.

[20] K. Svozil, "Quantum information via state partitions and the context translation principle," Journal of Modern Optics **51**, 811–819 (2004). quant-ph/0308110.

[21] N. D. Mermin, "Hidden variables and the two theorems of John Bell," Reviews of Modern Physics **65**, 803–815 (1993). URL `http://dx.doi.org/10.1103/RevModPhys.65.803`.

[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. Phil. Soc. **124**, 323–338 (1980). Reprinted in [24, pp. 152-167].

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

(a)

(b)

(c)

(d)

(e)

(f)

FIG. 3: Pictures of (a) the catwalk; (b) the author with two eyeglasses, one green and one red; (c) a "quant" crossing the catwalk; (d) agent obstacles in the "quantum" catwalk; (e) another "quant" crossing the catwalk; (f) hissing the flag.