Chocolate cryptography

Karl Svozil[*]

Institute for Theoretical Physics, Vienna University of Technology,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

Abstract

Some quantum cryptographic protocols can be implemented with specially prepared chocolate balls, others protected by value indefiniteness cannot. This latter feature, which follows from Bell- and Kochen-Specker type arguments, is only present in systems with three or more mutually exclusive outcomes. Conversely, there exist chocolate ball configurations utilizable for cryptography which cannot be realized by quantum systems.

PACS numbers: 03.67.Hk,03.65.Ud

Keywords: Quantum information, quantum cryptography, singlet states, entanglement, quantum nonlocality, value indefiniteness, contextuality

[*] svozil@tuwien.ac.at; http://tph.tuwien.ac.at/~svozil

I. QUANTUM RESOURCES FOR CRYPTOGRAPHY

Quantum cryptography [1] uses quantum resources to encode plain symbols forming some message. Thereby, the security of the code against cryptanalytic attacks to recover that message rests upon the validity of physics, giving new and direct meaning to Landauer's dictum [2] "information is physical."

What exactly are those quantum resources on which quantum cryptography is based upon? Consider, for a start, the following qualities of quantized systems:

(i) randomness of certain individual events, such as the occurrence of certain measurement outcomes for states which are in a superposition of eigenstates associated with eigenvalues corresponding to these outcomes;

(ii) complementarity, as proposed by Pauli, Heisenberg and Bohr;

(iii) value indefiniteness, as attested by Bell, Kochen & Specker, Greenberger, Horne and Zeilinger, and others (often, this property is referred to as "contextuality" [3–5]. Alas, contextual truth assignments are just one possibility among others to cope with the theorems mentioned, thereby providing a particular quasi-realistic, but not necessarily the only possible, "solution" or "interpretation" of those theorems [6]);

(iv) interference and quantum parallelism, allowing the co-representation of classically contradicting states of information by a coherent superposition thereof;

(v) entanglement of two or more particles, as pointed out by Schrödinger, such that their state cannot be represented as the product of states of the isolated, individual quanta, but is rather defined by the *joint* or *relative* properties of the quanta involved.

The first quantum cryptographic protocols, such as the ones by Wiesner [7] and Bennett & Brassard [8, 9], just require complementarity and random individual outcomes. This might be perceived ambivalently as an advantage – by being based upon only these two features – yet at the same time not utilizing the full mind boggling capacities of quantum mechanics, since they are not "protected" (in terms of no-go theorems for local noncontextual nonexotic [10, 11] hidden variable models not allowing) by Bell- or Kochen-Specker type [12–19] value indefiniteness.

This article addresses two issues: a critical re-evaluation of quantum cryptographic protocols in view of quantum value indefiniteness; as well as suggestions to improve them to assure the best possible protection "our" [20, p. 866] present quantum theory can afford. In doing so, a toy model will be introduced which implements complementarity but still is value definite. Then it will be exemplified how to do perform "quasi-classical" quantum-like cryptography with these models. Finally, methods will be discussed which go beyond the quasi-classical realm.

Even nowadays it is seldom acknowledged that, when it comes to value definiteness, there definitely *is* a difference between two- and three-dimensional Hilbert space. This difference can probably be best explained in terms of (conjugate) bases: whereas different bases in two-dimensional Hilbert space are disjoint and totally separated (they do not share any vector), from three dimensions onwards, they may share common elements. It is this inter-connectedness of bases and "frames" which supports both the Gleason and the Kochen-Specker theorems. This can, for instance, be used in derivations of the latter one in three dimensions, which effectively amount to a succession of rotations of bases along one of their elements (the original Kochen-Specker [13] proof uses 117 interlinked bases), thereby creating new rotated bases, until the original base is reached. Note that certain (even dense [11]) "dilutions" of bases break up the possibility to interconnect, thus allowing value definiteness.

The importance of these arguments for physics is this: since in quantum mechanics the dimension of Hilbert space is determined by the number of mutually exclusive outcomes, a *necessary* condition for a quantum system to be protected by value indefiniteness thus is that the associated quantum system has *at least three* mutually exclusive outcomes; two outcomes are insufficient for this purpose. Of course, one could argue that systems with two outcomes are still protected by complementarity.

II. REALIZATIONS OF QUANTUM CRYPTOGRAPHIC PROTOCOLS

Let us, for the sake of demonstration, discuss a concrete "toy" system which features complementarity but (not) value (in)definiteness. It is based on the partitions of a set. Suppose the set is given by $S = \{1, 2, 3, 4\}$, and consider two of its equipartitions $A = \{\{1, 2\}, \{3, 4\}\}$ and $B = \{\{1, 3\}, \{2, 4\}\}$, as well as the usual set theoretic operations (intersection, union and complement) and the subset relation among the elements of these two partitions. Then A and

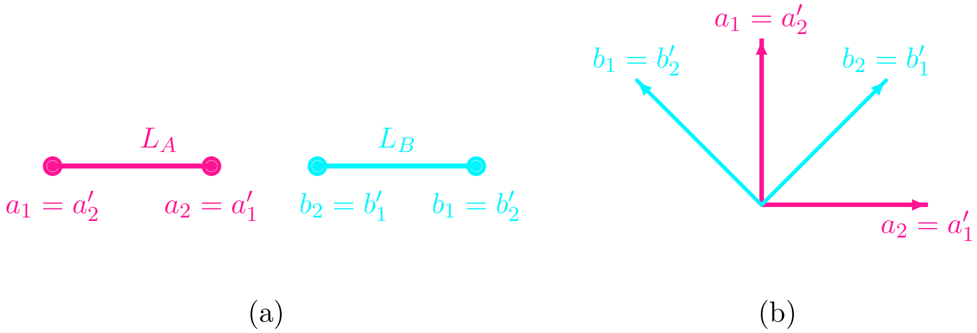

FIG. 1. (Color online) (a) Greechie diagram of $L_{A,B}$, consisting of two separate Boolean subalgebras L_A and L_B; (b) two-dimensional configuration of spin-$\frac{1}{2}$ state measurements along two noncollinear directions. As there are only two mutually exclusive outcomes, the dimension of the Hilbert space is two.

B generate two Boolean algebras $L_A = \{\emptyset, \{1,2\}, \{3,4\}, S\}$ and $L_B = \{\emptyset, \{1,3\}, \{2,4\}, S\}$ which are equivalent to a Boolean algebra with two atoms $a_1 = \{1,2\}$ & $a_2 = \{3,4\}$, as well as $b_1 = \{1,3\}$ & $b_2 = \{2,4\}$ per algebra, respectively. Then, the partition logic [6, 21, 22] consisting of two Boolean subalgebras $L_A \oplus L_B = L_{A,B} = \langle \{L_A, L_B\}, \cap, \cup, ', \subset \rangle$ is obtained as a pasting construction (through identifying identical elements of subalgebras [23–25]) from L_A and L_B: only elements contribute which are in L_A, or in L_B, or in both of them (i.e. in $L_A \cap L_B$) – the atoms of this algebra being the elements $a_1, \ldots, b_2$ – and all common elements. In the present case only the smallest and greatest elements $\emptyset$ and S – are identified. $L_{A,B}$ "inherits" the operations and relations of its subalgebras (also called *blocks* or *contexts*) L_A and L_B. This pasting construction yields a nondistributive and thus nonboolean, orthocomplemented propositional structure [25, 26]. Nondistributivity can quite easily be proven, as $a_1 \wedge (b_1 \vee b_2) \neq (a_1 \wedge b_1) \vee (a_1 \wedge b_2)$, since $b_1 \vee b_2 = S$, whereas $a_1 \wedge b_1 = a_1 \wedge b_2 = \emptyset$. Note that, although $a_1, \ldots, b_2$ are compositions of elements of S, not all elements of the power set of S associated with a Boolean algebra with four atoms, such as $\{1\}$ or $\{1,2,3\}$, are contained in $L_{A,B}$.

Figure 1(a) depicts a Greechie (orthogonality) diagram [23] of $L_{A,B}$, which represents elements in a Boolean algebra as single smooth curves; in this case there are just two atoms (least elements above $\emptyset$) per subalgebra; and both subalgebras are not interconnected.

Several realizations of this partition logic exist; among them

(i) the propositional structure [21, 27] of spin state measurements of a spin-$\frac{1}{2}$ particle along two noncollinear directions, or of the linear polarization of a photon along two nonorthogonal, noncollinear directions. A two-dimensional Hilbert space representation of this configuration is depicted in Figure 1(b). Thereby, the choice of the measurement direction decides which one of the two complementary spin state observables is measured;

(ii) generalized urn models [28, 29] utilizing black balls painted with two or more symbols in two or more colors. Suppose, for instance, just two symbols "0" and "1" in just two colors, say, "pink" and "light blue", resulting in four types of conceivable balls: 00, 01, 10, as well as 11 — many copies of which are randomly distributed in an urn. Suppose further that the experimenter looks at them with one of two differently colored eyeglasses, each one ideally matching the colors of only one of the symbols, such that only light in this wave length passes through. Thereby, the choice of the color decides which one of the two complementary observables associated with "pink" and "light blue" is measured. Propositions refer to the possible ball types drawn from the urn, given the information printed in the chosen color.

(iii) initial state identification problem for deterministic finite (Moore or Mealy) automata in an unknown initial state [22, 30]; in particular ones $\langle S, I, O, \delta, \lambda \rangle$ with four internal states $S = \{1, 2, 3, 4\}$, two input and two output states $I = O = \{0, 1\}$, an "irreversible" (all-to-one) transition function $\delta(s, i) = 1$ for all $s \in S$, $i \in I$, and an output function "modelling" the state partitions by $\lambda(1, 0) = \lambda(2, 0) = 0$, $\lambda(3, 0) = \lambda(4, 0) = 1$, $\lambda(1, 1) = \lambda(3, 1) = 0$, $\lambda(2, 1) = \lambda(4, 1) = 1$. Thereby, the choice of the input symbol decides which one of the two complementary observables is measured.

Let us, for the moment, consider generalized urn models, because they allow a "pleasant" representation as chocolate balls coated in black foils and painted with color symbols. With the four types of chocolate balls 00, 01, 10, and 11 drawn from an urn it is possible to execute the 1984 Bennett-Brassard (BB84) protocol [8, 9] and "generate" a secret key shared by two parties [31]. Formally, this reflects (i) the random draw of balls from an urn, as well as (ii) the complementarity modeled *via* the color painting and the colored eyeglasses. It also reflects the possibility to embed this model into a bigger Boolean (and thus classical) algebra 2^4 by "taking off the eyeglasses" and looking at both symbols of those four balls types simultaneously. The atoms of this Boolean algebra are just the ball types, associated with the four cases 00, 01, 10, and 11. The possibility of a classical embedding is also reflected in a "sufficient" number (i.e., by a separating, full set) of two-valued, dispersionless (only the sharp values "0" and "1" are allowed) states $P(a_1) + P(a_2) = P(b_1) + P(b_2) = 1$, with $P(x) \in \{0, 1\}$. These two-valued states can also be interpreted as logical truth assignments, irrespective of whether the observables have been (co-)measured.

When comparing BB84-type cryptography with quanta and chocolate balls, one has to keep in mind that the similarities with respect to complementarity appear somewhat superficial with regards to the state of the objects communicated *after* any measurement. Because even if an eavesdropper, say Eve, sticks to the rules of the game by putting on colored eyeglasses, any of her measurements would not affect or change the type of ball, and thus would not cause any *disturbance* of the objects communicated, thereby not causing any measurement errors between Alice and Bob. This is different from quantum complementarity and quantum cryptography protected by it, for if Eve would choose a different observable than Bob she would inevitably alter the state transferred. This amounts to a disturbance which makes it possible for Alice and Bob to recognize Eve's cryptanalytic attack through occasional measurement errors; at least if Eve is incapable of controlling the classical channel between the two. Of course one could alleviate this deficiency of the quasi-classical analogue by requiring Eve not to communicate the original object received from Bob, but by redrawing from the urn and sending Alice another object consistent with Eve's measurement.

The possibility to ascribe certain "ontic states" interpretable as observer-independent "omniscient elements of physical reality" (in the sense of Einstein, Podolsky and Rosen [32, p. 777], a paper which amazingly contains not a single reference) even for complementarity observables may raise some skepticism or even outright rejection, since that is not how quantum mechanics is known to perform at its most mind-boggling mode. Indeed, so far, the rant presented merely attempted to convince the reader that one can have complementarity *as well as* value definiteness; i.e., complementarity is not sufficient for value indefiniteness in the sense of the Bell- and Kochen-Specker argument.

Unfortunately, the two-dimensionality of the associated Hilbert space is also a feature plaguing present random number generators based on beam splitters [33–36]. In this respect, most of the present random number generators using beam splitters are protected by the randomness of single outcomes as well as by complementarity, but not by certified value indefiniteness [37–40], as guaranteed by quantum theory in its standard form [41]. Their methodology should also be improved by the methods discussed below.

III. SUPPORTING CRYPTOGRAPHY WITH VALUE INDEFINITENESS

Fortunately, quantum mechanics is more resourceful and mind-boggling than that, as it does not permit any two-valued states which may be ontologically interpretable as elements of physical reality. So we have to go further, reminding ourselves that value indefiniteness comes about only for Hilbert spaces of dimensions three and higher. There are several ways of doing this. The following options will be discussed:

(i) the known protocols can be generalized to three or more outcomes [37];

(ii) entangled pairs of particles [42] associated with statistical value indefiniteness may be considered;

(iii) full, nonprobabilistic value indefiniteness may be attempted, at least counterfactually.

A. Generalizations to three and more outcomes

In constructing quantum random number generators *via* beam splitters which ultimately are used in cryptographic setups, it is important (i) to have full control of the particle source, and (ii) to use beam splitters with three or more output ports, associated with three- or higher-dimensional Hilbert spaces. Thereby, the question of whether it is *sufficient* for this purpose to compose a multiport beam splitter by a succession of phase shifters and beam splitters with two output ports [43, 44], based on elementary decompositions of the unitary group [45] remains to be answered.

Dichotomic sequences could be obtained from sequences containing more than two symbols by discarding all other symbols from that sequence [46], or by identifying the additional symbols with one (or both) of the two symbols. For standard normalization procedures and their issues, the reader is referred to Refs. [47–52].

One concrete realization would be a spin-$\frac{3}{2}$ particle. Suppose it is prepared in one of its four spin states, say the one associated with angular momentum $+\frac{3}{2}\hbar$ in some arbitrary but definite direction; e.g., by a Stern-Gerlach device. Then, its spin state is again measured along a perpendicular direction; e.g., by another, differently oriented, Stern-Gerlach device. Two of the output ports, say the ones corresponding to positive angular momentum $+\frac{3}{2}\hbar$ and $+\frac{1}{2}\hbar$, are identified with the symbol "0," the other two ports with the symbol "1." In that way, a random sequence is obtained from quantum coin tosses which can be ensured to operate under the conditions of value indefiniteness in the sense of the Kochen-Specker theorem. Of course, this protocol can also be used to generate random sequences containing four symbols (one symbol per detector).

With respect to the use of beam splitters, the reader is kindly reminded of another issue related to the fact that beam splitters are *reversible* devices capable of only translating an incoming signal into an outgoing signal in a *one-to-one* manner. The "nondestructive" action of a beam splitter could also be demonstrated by "reconstructing" the original signal through a "reversed" identical beam splitter in a Mach-Zehnder interferometer [53]. In this sense, the signal leaving the output ports of a beam splitter is "as good" for cryptographic purposes as the one entering the device. This fact relegates considerations of the quality of quantum randomness to the quality of the source. Every care should thus be taken in preparing the source to assure that the state entering the input port (i) either is pure and could subsequently be used for measurements corresponding to conjugate bases, (ii) or is maximally mixed, resulting in a representation of its state in finite dimensions proportional to the unit matrix.

B. Configurations with statistical value indefiniteness

Protocols like the Ekert protocol [42] utilize two entangled two-state particles for a generation of a random key shared by two parties. The particular Einstein-Podolsky-Rosen configuration [32] and the singlet Bell state communicated among the parties guarantee stronger-than-classical correlations of their sequences, resulting in a violation of Bell-type inequalities obeyed by classical probabilities.

Although criticized [54] on the grounds that the Ekert protocol in certain cryptanalytic aspects is equivalent to existing ones (see Ref. [55] for a reconciliation), it offers additional security in the light of quantum value indefiniteness, as it suggests to probe the nonclassical parts of quantum statistics. This can best be understood in terms of the impossibility to generate co-existing tables of all – even the counterfactually possible – measurement outcomes of the quantum observables used [56]. This, of course, can only happen for the four-dimensional Hilbert space configuration proposed by Ekert, and not for effectively two-dimensional ones of previous proposals. As a result, if the Ekert protocol would be executed with chocolate balls instead of suitable quanta, the data would not violate the classical bounds predicted by quantum theory, thereby dissatisfying essential criteria thereof. In this respect the Ekert protocol fails for chocolate balls, thereby indicating potential cryptanalytic risks. Formally, this is due to the nonexistence of two-valued states in four-dimensional Hilbert space.

Suppose one would nevertheless attempt to "mimic" an Ekert type protocol proposed by Bennett, Brassard and Mermin (BBM92) [54] with a classical "singlet" state which uses compositions of two balls of the form 00—11 / 01—10 / 10—01 / 11—00, with strictly different (alternatively strictly identical) particle types. The resulting probabilities and expectations would obey the classical Clauser-Horne-Shimony-Holt bounds [57]. This is due to the fact that generalized urn models have quasi-classical probability distributions which can be represented as convex combinations of the full set of separable two-valued states on their observables.

C. Nonprobabilistic value indefiniteness

In an attempt to fully utilize quantum value indefiniteness, we propose a generalization of the BB84 protocol on a propositional structure which does not allow any two-valued state. In principle, this could be any kind of finite configuration of observables in three- and higher-dimensional Hilbert space; in particular ones which have been proposed for a proof of the Kochen-Specker theorem.

For the sake of a concrete example, we shall consider a variant of the tightly interlinked collection of observables in four-dimensional Hilbert space presented by Cabello, Estebaranz and García-Alcaine [58, 59], which is depicted in Figure 2. (Their original configuration would also suffice for the following argument.) Instead of two measurement bases of two-dimensional Hilbert space used in the BB84 protocol, 15 such bases of four-dimensional Hilbert space, corresponding to the 15 smooth (unbroken) orthogonal curves in Fig. 2 are used. In what follows, it is assumed that any kind of random decision has been prepared according to the protocol for generating random sequences sketched above.

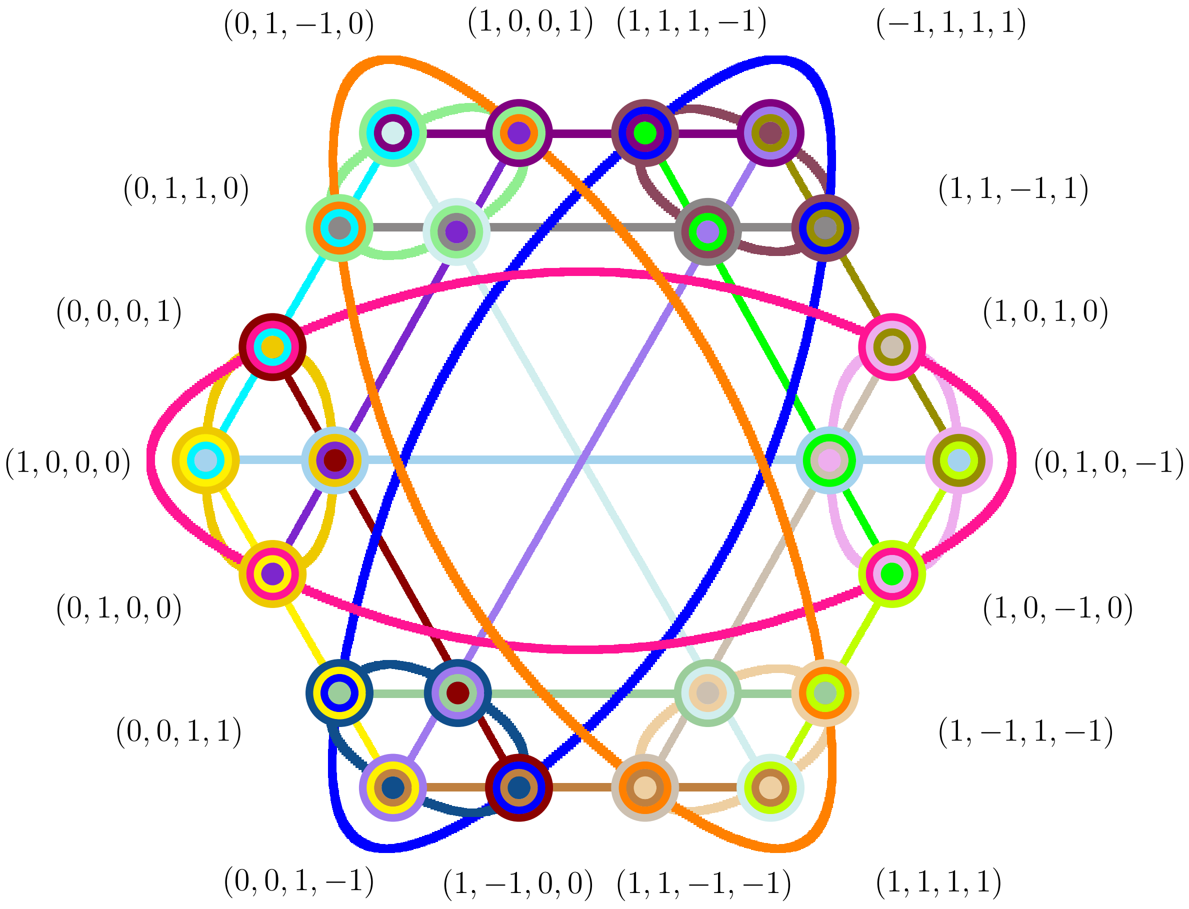

FIG. 2. (Color online) Greechie orthogonality diagram of a “short” proof [58, 59] of the Kochen-Specker theorem in four dimensions containing 24 vectors whose linear span can be identified with propositions [27] in 24 tightly interlinked contexts [60]. The graph cannot be colored by the two colors red (associated with truth) and green (associated with falsity) such that every context contains exactly one red and three green points. For the sake of a proof, consider just the six outer lines and the three outer ellipses. Indeed, in a table containing the points of the contexts as columns and the enumeration of contexts as rows, every red point occurs in exactly *four* contexts, and there should be an *even* number of red points. On the other hand, there are 15 contexts involved; thus by the rules it follows that there should be an *odd* number (15) of red points in this table (exactly one per context).

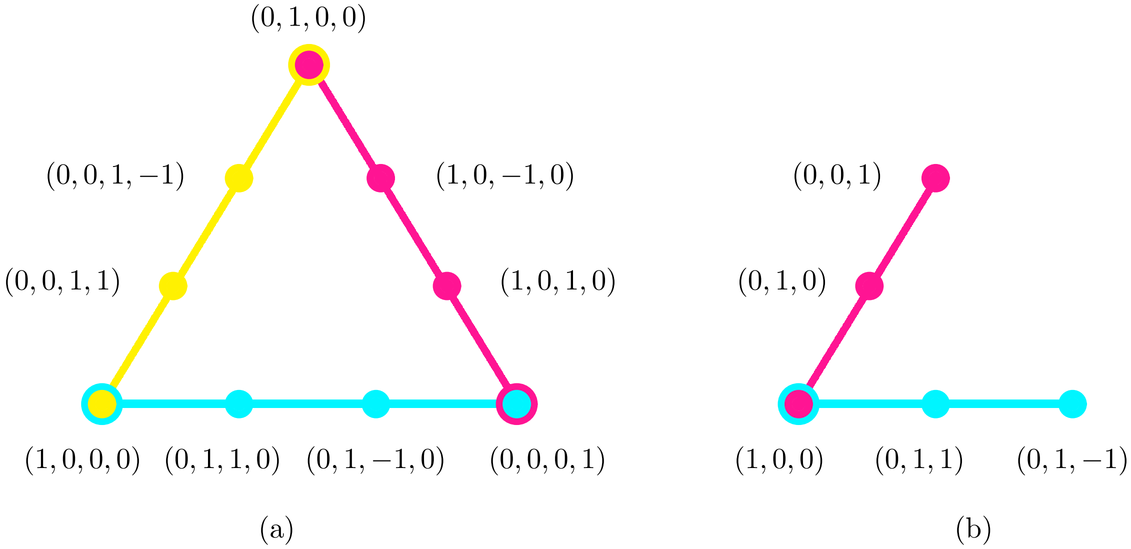

FIG. 3. (Color online) Subdiagrams of Figure 2 allowing (value definite) chocolate ball realizations.

(i) In the first step, "Alice" randomly picks an arbitrary basis from the 15 available ones, and sends a random state to "Bob."

(ii) In the second step, Bob independently from Alice, picks some (not necessarily different from Alice's) basis at random, and measures the particle received from Alice.

(iii) In the third step, Alice and Bob compare their bases over a public channel, and keep only those events which were recorded either in a common basis, or in an observable interlinking two different bases.

(iv) Both then exchange some of the matching outcomes over a public channel to assure that nobody has attended their quantum channel.

(v) Bob and Alice encode the four outcomes by four or less different symbols. As a result, Bob and Alice share a common random key certified by quantum value indefiniteness.

The advantage of this protocol resides in the fact that it does not allow its realization by any partition of a set, or any kind of colored chocolate balls. Because if it did, any such coloring could be used to generate "classical" two-valued states, which in turn may be used towards a classical re-interpretation of the quantum observables; an option ruled out by the Kochen-Specker theorem.

Readers not totally convinced at this point might, for the sake of demonstration, consider a generalized urn model with 15 colors, associated with the 15 bases in Figure 2. Suppose further that there is a uniform set of symbols, say $\{0,1,2,3\}$ for all four colors. If all varieties (permutations) contribute, the number of different types of balls should be 4^9. Note, however, that every interlinked color must have *identical* symbols in the interlinking colors; a condition which cannot be satisfied globally for all the interlinks in Figure 2.

For the sake of an explicit demonstration, a simplified version of the protocol, which is based on a subdiagram of Figure 2, contains only three contexts, which are closely interlinked. The structure of observables is depicted in Figure 3(a). The vectors represent observables in four-dimensional Hilbert space in their usual interpretation as projectors generating the one-dimensional subspaces spanned by them. In addition to this quantum mechanical representation, and in contrast to the Kochen-Specker configuration in Figure 2, this global collection of observables still allows for value definiteness, as there are "enough" two valued states permitting the formation of a partition logic and thus a chocolate ball realization; e.g.,

$$\begin{gathered}\{\{\{1,2\},\{3,4,5,6,7\},\{8,9,10,11,12\},\{13,14\}\},\\ \{\{1,4,5,9,10\},\{2,6,7,11,12\},\{3,8\},\{13,14\}\},\\ \{\{1,2\},\{3,8\},\{4,6,9,11,13\},\{5,7,10,12,14\}\}\}.\end{gathered}$$

The three partitions of the set $\{1,2,\ldots,14\}$ have been obtained by indexing the atoms in terms of all the nonvanishing two-valued states on them [6, 22], as depicted in Figure 4. They can be straightforwardly applied for a chocolate ball configuration with three colors (say green, red and blue) and four symbols (say 0, 1, 2, and 3). The 14 ball types corresponding to the 14 different two-valued measures are as follows: 000, 010, 121, 102, 103, 112, 113, 221, 202, 203, 212, 213, 332, and 333.

Figure 3(b) contains a three-dimensional subconfiguration with two complementary contexts interlinked in a single observable. It again has a value definite representation in terms of partitions of a set, and thus again a chocolate ball realization with three symbols in two colors; e.g., 00, 11, 12, 21, and 22.

IV. NONCOMMUTATIVE CHOCOLATE CRYPTOGRAPHY WHICH CANNOT BE REALIZED QUANTUM MECHANICALLY

Quantum mechanics does not allow a "triangular" structure of observables similar to the one depicted in Fig. 3 with *three* instead of four atoms per block (context), since no geometric

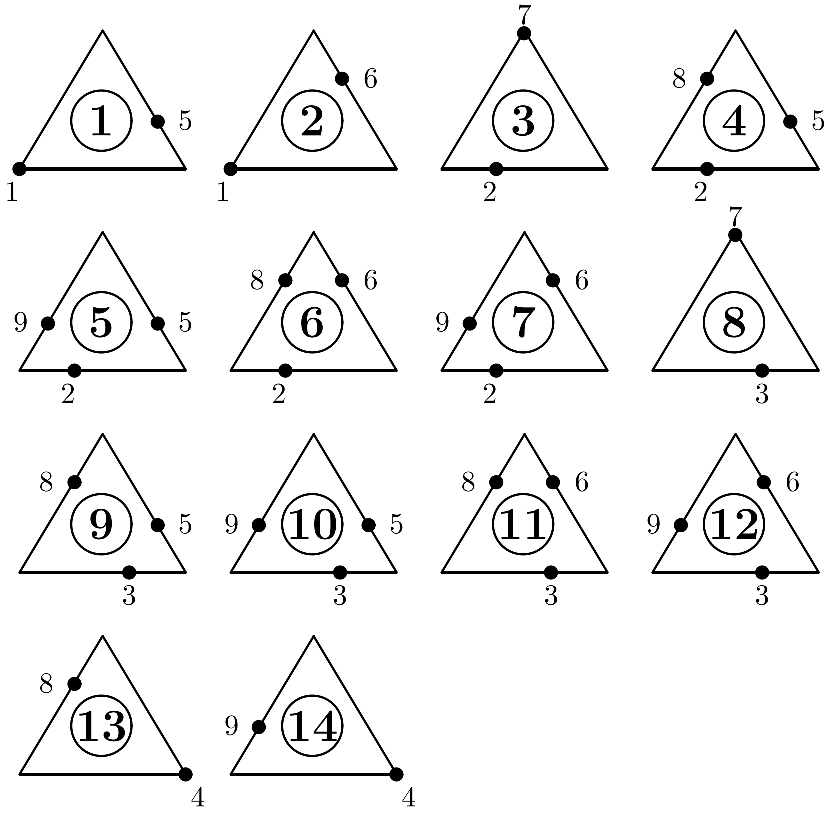

FIG. 4. Two-valued states interpretable as global truth functions of the observables depicted in Figure 3(a). Encircled numbers count the states, smaller numbers label the observables.

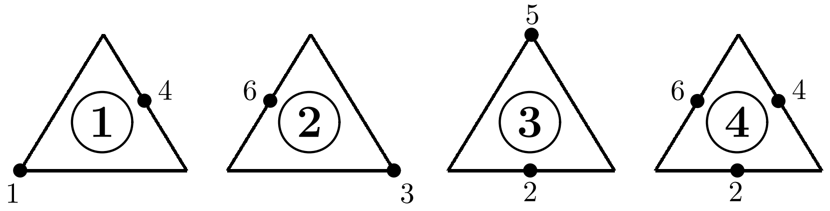

FIG. 5. Two-valued states on triangular propositional structure with three atoms per context or block.

configuration of tripods exist in three-dimensional vector space which would satisfy this scheme. (For a different propositional structure not expressible by quantum mechanics, see Specker's programmatic article [12] from 1960.) It contains six atoms $1, \ldots, 6$ in the blocks 1–2–3, 3–4–5, 5–6–1. In order to obtain a partition logic on which the chocolate ball model can be based, the four two-valued states are enumerated and depicted in Figure 5.

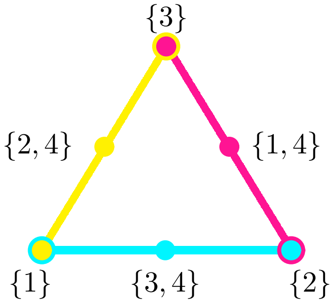

FIG. 6. (Color online) Propositional structure allowing (value definite) chocolate ball realizations with three atoms per context or block which does not allow a quantum analogue.

The associated partition logic is given by

$$\begin{gathered}\{\{\{1\},\{2\},\{3,4\}\},\\ \{\{1,4\},\{2\},\{3\}\},\\ \{\{1\},\{2,4\},\{3\}\}\}.\end{gathered}$$

Every one of the three partitions of the set $\{1,\ldots,4\}$ of ball types labeled by 1 through 4 corresponds to a color; and there are three symbols per colors. For the first (second/third) partition, the propositions associated with these protocols are:

- "when seen through light of the first (second/third) color (e.g., pink/light blue/yellow), symbol "0" means ball type number 1 (2/3);"

- "when seen through light of the first (second/third) color (e.g., pink/light blue/yellow), symbol "1" means ball type number 3 or 4 (1 or 4/2 or 4);"

- "when seen through light of the first (second/third) color (e.g., pink/light blue/yellow), symbol "2" means ball type number 2 (3/1)."

More explicitly, there are four ball types of the form 012, 201, 120, and 111. The resulting propositional structure is depicted in Fig. 6. With respect to conceivable realizations, cryptographic protocols – such as the one sketched above – based on this structure are "stranger than quantum mechanical" ones.

V. SUMMARY AND DISCUSSION

It has been argued that value indefiniteness rather than complementarity should be used as a quantum resource against cryptanalytic attacks. One reason for this suggestion is that certain types of complementarity can be mimicked by quasi-classical configurations, whereas there cannot exist a noncontextual (quasi-)classical analogue of quantum value indefiniteness.

The formal reason for the impossibility of (quasi-)classical models in the latter case is the nonexistence of any two-valued measures on the propositional structure resulting from the associated observables; at least with the assumptions (e.g. noncontextuality) made. Constructive proofs (by contradiction) of this formal result has yielded Kochen-Specker type theorems [12–19]. By contrast, quantum complementarity may still allow observables and propositional structures with a sufficient number of two-valued states to even allow a homeomorphic embedding into a classical Boolean algebra [21]. Configurations associated with merely statistical violations of Bell-type inequalities are in-between those two extremes because they still allow "a few" two-valued states which can be used for the coloring of certain types of chocolate balls; however these states are insufficient to render a faithful embedding into Boolean algebras, and at the same time incapable of rendering the quantum violations of the associated Bell-type inequalities. If in such cases one insists in tabling potential physical properties, these have to be contextual [61]. Thus quantitatively – that is in terms of the necessary violations of noncontextuality – some of the protocols suggested here, by explicitly using Kochen-Specker type constructions, utilize even "more" nonclassical resources of quantum mechanics than the Ekert protocol based on Bell-type inequalities.

Whether this "sharpening" of nonclassicality can be considered an improvement over previous cryptographic protocols remains conjectural. It may be objected that quantum complementarity suffices as resource against cryptanalytic attacks, and thus the original BB84 protocol needs not be amended. Because if one accepts quantum complementarity as an axiom, there is no necessity for any further "improvement" of security against cryptanalytic attacks. To this criticism I respond with a performance of the original BB84 protocols with chocolate balls [31]; or more formally, by stating that configurations with just two outcomes leave open the possibility of a quasi-classical explanation, as they cannot rule out the existence of sufficiently many two-valued states in order to construct homeomorphisms, that is, structure-preserving maps between the quantum and classical observables. A necessary condition for the quantum resource of value indefiniteness or contextuality is the presence of at least three mutually exclusive outcomes. But even then, no proof of unconditional security of the new protocols can be given.

From a purely operational, phenomenological point of view, all that can be measured are violations of certain statistical predictions. There does not exist any direct way of simultaneously testing this nonclassical quantum behavior on individual particles [62], even in the Kochen-Specker [59, 63] or Greenberger-Horne-Zeilinger [64, 65] type configurations. Nevertheless, in other research areas, such as for instance with regard to quantum random number generators, the additional security gained by monitoring value indefiniteness or contextuality is often perceived as an advantage [37–40]. In this sense, the new protocol may present some advantage over the BB84, and even the Ekert protocols. Thus when it comes to fully harvesting the quantum, it might not be too unreasonable to utilize value indefiniteness, one of its most "mind-boggling" features encountered if one assumes the physical relevance of nonoperational yet counterfactual observables.

Acknowledgements

The author gratefully acknowledges discussions with Cristian Calude and Josef Tkadlec, as well as the criticism, comments and suggestions of two anonymous Referees. He also enjoyed the kind hospitality of the *Centre for Discrete Mathematics and Theoretical Computer Science (CDMTCS)* of the *Department of Computer Science at The University of Auckland* where this manuscript has been conceived. This work was also supported by *The Department for International Relations* of the *Vienna University of Technology.* The pink–light blue–yellow coloring scheme is by Renate Bertlmann; communicated to the author by Reinhold Bertlmann.

[1] In view of the many superb presentations of quantum cryptography — to name but a few, see Refs. [66, 67] and [68, Chapter 6] (or, alternatively, [69, Section 6.2]), as well as [70, Section 12.6]; apologies to other authors for this incomplete, subjective collection — I refrain from any extensive introduction.

[2] Rolf Landauer, "Information is physical," Physics Today **44**, 23–29 (1991).

[3] Niels Bohr, "Discussion with Einstein on epistemological problems in atomic physics," in *Albert Einstein: Philosopher-Scientist*, edited by P. A. Schilpp (The Library of Living Philosophers, Evanston, Ill., 1949) pp. 200–241.

[4] John S. Bell, "On the problem of hidden variables in quantum mechanics," Reviews of Modern Physics **38**, 447–452 (1966).

[5] Michael Redhead, *Incompleteness, Nonlocality, and Realism: A Prolegomenon to the Philosophy of Quantum Mechanics* (Clarendon Press, Oxford, 1990).

[6] Karl Svozil, "Contexts in quantum, classical and partition logic," in *Handbook of Quantum Logic and Quantum Structures*, edited by Kurt Engesser, Dov M. Gabbay, and Daniel Lehmann (Elsevier, Amsterdam, 2009) pp. 551–586, arXiv:quant-ph/0609209.

[7] Stephen Wiesner, "Conjugate coding," SIGACT News **15**, 78–88 (1983).

[8] 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.

[9] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin, "Experimental quantum cryptography," Journal of Cryptology **5**, 3–28 (1992).

[10] Itamar Pitowsky, "Resolution of the Einstein-Podolsky-Rosen and Bell paradoxes," Physical Review Letters **48**, 1299–1302 (1982).

[11] David A. Meyer, "Finite precision measurement nullifies the Kochen-Specker theorem," Physical Review Letters **83**, 3751–3754 (1999), quant-ph/9905080.

[12] Ernst Specker, "Die Logik nicht gleichzeitig entscheidbarer Aussagen," Dialectica **14**, 239–246 (1960), http://arxiv.org/abs/1103.4537.

[13] Simon Kochen and Ernst P. Specker, "The problem of hidden variables in quantum mechanics," Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal) **17**, 59–87 (1967).

[14] Neal Zierler and Michael Schlessinger, "Boolean embeddings of orthomodular sets and quantum logic," Duke Mathematical Journal **32**, 251–262 (1965).

[15] Václav Alda, "On 0-1 measures for projectors I," Aplikace matematiky (Applications of Mathematics) **25**, 373–374 (1980).

[16] Václav Alda, "On 0-1 measures for projectors II," Aplikace matematiky (Applications of

Mathematics) **26**, 57–58 (1981).

[17] Franz Kamber, “Die Struktur des Aussagenkalküls in einer physikalischen Theorie,” Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse **10**, 103–124 (1964).

[18] Franz Kamber, “Zweiwertige Wahrscheinlichkeitsfunktionen auf orthokomplementären Verbänden,” Mathematische Annalen **158**, 158–196 (1965).

[19] N. D. Mermin, “Hidden variables and the two theorems of John Bell,” Reviews of Modern Physics **65**, 803–815 (1993).

[20] Max Born, “Zur Quantenmechanik der Stoßvorgänge,” Zeitschrift für Physik **37**, 863–867 (1926).

[21] Karl Svozil, *Quantum Logic* (Springer, Singapore, 1998).

[22] Karl Svozil, “Logical equivalence between generalized urn models and finite automata,” International Journal of Theoretical Physics **44**, 745–754 (2005), quant-ph/0209136.

[23] J. R. Greechie, “Orthomodular lattices admitting no states,” Journal of Combinatorial Theory **10**, 119–132 (1971).

[24] Mirko Navara and Vladimír Rogalewicz, “The pasting constructions for orthomodular posets,” Mathematische Nachrichten **154**, 157–168 (1991).

[25] Gudrun Kalmbach, “Omologic as a Hilbert type calculus,” in *Current Issues in Quantum Logic*, edited by E. Beltrametti and Bas C. van Fraassen (Plenum Press, New York, 1981) p. 333.

[26] Pavel Pták and Sylvia Pulmannová, *Orthomodular Structures as Quantum Logics* (Kluwer Academic Publishers, Dordrecht, 1991).

[27] Garrett Birkhoff and John von Neumann, “The logic of quantum mechanics,” Annals of Mathematics **37**, 823–843 (1936).

[28] Ron Wright, “Generalized urn models,” Foundations of Physics **20**, 881–903 (1990).

[29] Anatolij Dvurečenskij, Sylvia Pulmannová, and Karl Svozil, “Partition logics, orthoalgebras and automata,” Helvetica Physica Acta **68**, 407–428 (1995).

[30] Edward F. Moore, “Gedanken-experiments on sequential machines,” in *Automata Studies*, edited by C. E. Shannon and J. McCarthy (Princeton University Press, Princeton, NJ, 1956) pp. 129–153.

[31] Karl Svozil, “Staging quantum cryptography with chocolate balls,” American Journal of

Physics **74**, 800–803 (2006), physics/0510050.

[32] Albert Einstein, Boris Podolsky, and Nathan Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Physical Review **47**, 777–780 (1935).

[33] Karl Svozil, "The quantum coin toss—testing microphysical undecidability," Physics Letters A **143**, 433–437 (1990).

[34] J. G. Rarity, M. P. C. Owens, and P. R. Tapster, "Quantum random-number generation and key sharing," Journal of Modern Optics **41**, 2435–2444 (1994).

[35] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger, "A fast and compact quantum random number generator," Review of Scientific Instruments **71**, 1675–1680 (2000), quant-ph/9912118.

[36] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden, "Optical quantum random number generator," Journal of Modern Optics **47**, 595–598 (2000).

[37] Helle Bechmann-Pasquinucci and Asher Peres, "Quantum cryptography with 3-state systems," Physical Review Letters **85**, 3313–3316 (2000).

[38] Cristian S. Calude and Karl Svozil, "Quantum randomness and value indefiniteness," Advanced Science Letters **1**, 165–168 (2008), arXiv:quant-ph/0611029.

[39] Karl Svozil, "Three criteria for quantum random-number generators based on beam splitters," Physical Review A **79**, 054306 (2009), arXiv:quant-ph/0903.2744.

[40] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).

[41] John von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, 1932) English translation in Ref. [71].

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

[43] M. Reck, Anton Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," Physical Review Letters **73**, 58–61 (1994).

[44] Karl Svozil, "Noncontextuality in multipartite entanglement," J. Phys. A: Math. Gen. **38**, 5781–5798 (2005), quant-ph/0401113.

[45] F. D. Murnaghan, *The Unitary and Rotation Groups* (Spartan Books, Washington, D.C., 1962).

[46] Cristian Calude and Ion Chiţescu, "Qualitative properties of P. Martin-Löf random sequences," Unione Matematica Italiana. Bollettino. B. Serie VII **3**, 229–240 (1989).

[47] John von Neumann, "Various techniques used in connection with random digits," National Bureau of Standards Applied Math Series **12**, 36–38 (1951), reprinted in *John von Neumann, Collected Works, (Vol. V)*, A. H. Traub, editor, MacMillan, New York, 1963, p. 768–770.

[48] Paul A. Samuelson, "Constructing an unbiased random sequence," Journal of the American Statistical Association **63**, 1526–1527 (1968).

[49] Peter Elias, "The efficient construction of an unbiased random sequence," Ann. Math. Statist. **43**, 865–870 (1972).

[50] Yuval Peres, "Iterating Von Neumann's procedure for extracting random bits," The Annals of Statistics **20**, 590–597 (1992).

[51] Markus Dichtl, "Bad and good ways of post-processing biased physical random numbers," in *Fast Software Encryption. Lecture Notes in Computer Science Volume 4593/2007*, edited by Alex Biryukov (Springer, Berlin and Heidelberg, 2007) pp. 137–152, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers.

[52] Patrick Lacharme, "Post-processing functions for a biased physical random number generator," in *Fast Software Encryption. Lecture Notes in Computer Science Volume 5086/2008*, edited by Kaisa Nyberg (Springer, Berlin and Heidelberg, 2008) pp. 334–342, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers.

[53] Daniel M. Greenberger, Mike A. Horne, and Anton Zeilinger, "Multiparticle interferometry and the superposition principle," Physics Today **46**, 22–29 (1993).

[54] Charles H. Bennett, Gilles Brassard, and David N. Mermin, "Quantum cryptography without Bell's theorem," Physical Review Letters **68**, 557–559 (1992).

[55] Charles H. Bennett, Gilles Brassard, and Artur K. Ekert, "Quantum cryptography," Scientific American **267**, 50–57 (1992).

[56] Asher Peres, "Unperformed experiments have no results," American Journal of Physics **46**, 745–747 (1978).

[57] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt, "Proposed experiment to test local hidden-variable theories," Physical Review Letters **23**, 880–884 (1969).

[58] Adán Cabello, José M. Estebaranz, and G. García-Alcaine, "Bell-Kochen-Specker theorem: A proof with 18 vectors," Physics Letters A **212**, 183–187 (1996).

[59] Adán Cabello, "Experimentally testable state-independent quantum contextuality," Physical Review Letters **101**, 210401 (2008).

[60] Josef Tkadlec, (2009), private communication.

[61] Karl Svozil, "How much contextuality?" Natural Computing **11**, 261–265 (2012), arXiv:1103.3980.

[62] Karl Svozil, "Are simultaneous Bell measurements possible?" New Journal of Physics **8**, 39, 1–8 (2006), quant-ph/0401113.

[63] G. Kirchmair, F. Zähringer, R. Gerritsma, M. Kleinmann, O. Gühne, A. Cabello, R. Blatt, and C. F. Roos, "State-independent experimental test of quantum contextuality," Nature **460**, 494–497 (2009), arXiv:0904.1655.

[64] Daniel M. Greenberger, Mike A. Horne, and Anton 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.

[65] Jian-Wei 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).

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

[67] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, "The security of practical quantum key distribution," Reviews of Modern Physics **81**, 1301–1350 (2009), arXiv:0802.4155.

[68] N. David Mermin, "Lecture notes on quantum computation," (2002-2008).

[69] N. David Mermin, *Quantum Computer Science* (Cambridge University Press, Cambridge, 2007).

[70] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[71] John von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, NJ, 1955).