Theoretical Computer Science 560 (2014) 82–90

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Non-contextual chocolate balls versus value indefinite quantum cryptography

Karl Svozil

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

ARTICLE INFO

Article history:
Received 4 December 2008
Accepted 11 May 2014
Available online 21 September 2014

Keywords:
Quantum information
Quantum cryptography
Singlet states
Entanglement
Quantum non-locality
Value indefiniteness
Contextuality

ABSTRACT

Some quantum cryptographic protocols can be implemented with specially prepared metaphorical chocolate balls representing local hidden variables, 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 local hidden variable models based on chocolate ball configurations utilizable for cryptography which cannot be realized by quantum systems. The possibility that quantum cryptography supported by value indefiniteness (contextuality) has practical advantages over more conventional quantum cryptographic protocols remains highly speculative.

1. 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 [36] "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 and Specker, Greenberger, Horne and Zeilinger, Pitowsky and others [1,2] (often, this property is referred to as "contextuality" [12,6,53]. 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 [64]);
(iv) interference and quantum parallelism, allowing the co-representation of classically contradicting states of information by a coherent superposition thereof;

E-mail address: svozil@tuwien.ac.at.
URL: http://tph.tuwien.ac.at/~svozil.

[1] In view of the many superb presentations of quantum cryptography — to name but a few, see Refs. [24,55] and [38, Chapter 6] (or, alternatively, [39, Section 6.2]), as well as [44, Section 12.6]; apologies to other authors for this incomplete, subjective collection — I refrain from any extensive introduction.

http://dx.doi.org/10.1016/j.tcs.2014.09.019
0304-3975/© 2014 Elsevier B.V. All rights reserved.

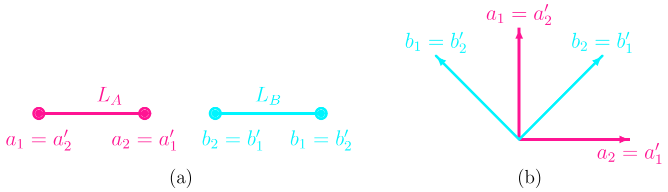

Fig. 1. (Color online.) (a) Greechie diagram of $L_{A,B}$, consisting of two separate Boolean subalgebras L_A and L_B; (b) two-dimensional Hilbert space configuration of spin-$\frac{1}{2}$ state measurements along two non-collinear directions. As there are only two mutually exclusive outcomes, the dimension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

(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 [71] and Bennett and Brassard [8,7], just require complementarity and random individual outcomes. It may well be that a different quantum cryptographic scheme that uses stronger or additional powers provided by quantum theory, such as value indefiniteness (or, by another term, contextuality) manifesting itself in Bell– or Kochen–Specker type theorems [56,34,73,3,4,31,32,37,49,28], will provide an advantage over these former protocols.

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 [34] proof uses 117 interlinked bases), thereby creating new rotated bases, until the original base is reached. Note that certain (even dense [40]) "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.

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" [13, 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.

2. 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 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 $a_1 = \{1, 2\}$ and $a_2 = \{3, 4\}$, as well as $b_1 = \{1, 3\}$ and $b_2 = \{2, 4\}$ per algebra, respectively. Then, the partition logic [59,60,64] 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 [25,43,30]) 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 $a_1, \dots, b_2$ – 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 non-distributive and thus non-boolean, orthocomplemented propositional structure [30,50]. 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 $a_1, \dots, b_2$ 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 $L_{A,B}$.

Fig. 1(a) depicts a Greechie (orthogonality) diagram [25] 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.