



ELSEVIER

Available online at www.sciencedirect.com



ScienceDirect

Electronic Notes in
Theoretical Computer
Science

Electronic Notes in Theoretical Computer Science 270 (2) (2011) 231–249

www.elsevier.com/locate/entcs

Graphical Calculus for Quantum Key Distribution (Extended Abstract)

Bob Coecke¹

Oxford University Computing Laboratory

Quanlong Wang²

[†]*LMIB, School of Mathematics and System Sciences
Beihang University, Beijing, P. R. China*

[‡]*State Key Laboratory of Information Security
(Graduate University of Chinese Academy of Sciences)*

Baoshan Wang² Yongjun Wang² Qiye Zhang²

*LMIB, School of Mathematics and System Sciences
Beihang University, Beijing, P. R. China*

Abstract

Controlled complementary measurements are key to quantum key distribution protocols, among many other things. We axiomatize controlled complementary measurements within symmetric monoidal categories, which provides them with a corresponding graphical calculus. We study the BB84 and Ekert91 protocols within this calculus, including the case where there is an intercept-resend attack.

Keywords: categorical semantics, quantum key distribution, complementary observables, graphical calculus.

1 Introduction

Guaranteeing security properties of communication protocols is highly non-trivial, as exemplified by the time it took to discover that the widely used Needham-

¹ Email: coecke@comlab.ox.ac.uk

² Email: qlwang, bwang, wangyj, zhangqiye@buaa.edu.cn

³ This work is partially supported by the National Science Foundation of China (NSFC) under Grants 60773141 and 10701006, by EPSRC Advanced Research Fellowship EP/D072786/1 and by US Office of Naval Research (ONR) Grant N00014-09-1-0248. We thank Samson Abramsky, Ross Duncan and Chris Heunen for constructive feedback.

Schroeder protocol was in fact insecure [19]. Consequently, modern research in the area involves high-level methods. While security of traditional public-key cryptography relies on the computational difficulty of certain mathematical functions and does not provide an indication of eavesdropping, in contrast, the security of quantum public-key cryptography relies on the foundations of quantum mechanics, and can detect eavesdropping by comparing bit by bit a subset of the data of the communicating parties. This paper is concerned with high-level methods for quantum public-key cryptography.

Over the past couple of years, several researchers have developed a high-level categorical formalization of quantum mechanics in terms of symmetric monoidal dagger categories, which comes with a corresponding graphical calculus e.g. [1,22,8,4,6]. These graphical calculi trace back to work by Penrose in the 1970's [21] and became a formal discipline with the work of Joyal and Street [16,23]. Particularly relevant for the categorical formalization of quantum mechanics are Kelly and Laplaza's *compact (closed) categories* [17], Carboni and Walters' Frobenius algebras [3] and Lack's analysis of their graphical representation [18]. All of these admit so-called *dagger*-versions [1,22,8], which account for the Hilbert space inner-product (and hence orthogonality).

Within the graphical calculus, quantum measurements [8,10], classically controlled quantum measurements [6] and complementary observables [4] can be given an intuitive axiomatization, which, in turns, provide intuitive descriptions of typical quantum protocols such as quantum teleportation [1,8,6], superdense coding [4], and several measurement-based quantum computational schemes such as Gottesman and Chuang's logic-gate teleportation [1], Perdrix' state-transfer [7] and Raussendorf and Briegel's one-way model [4,6,11].

Quantum cryptographic protocols such as BB84 and Ekert 91 [2,12] involve controlled complementary observables. While we do have graphical understanding of complementarity of two observables, as well as of controlled observables, in the latter the control space is an abstract one. Hence blending these two concepts into one is not straightforward. This is the main contribution of this paper: an axiomatization of controlled complementary measurements in the language of symmetric monoidal categories, and hence in terms of graphical calculus. This is done in Section 3. This enables us to give a concise presentation for the BB84 and Ekert 91 protocols. We prove the correctness of these, and analyze the case where there is an intercept-resend attack. This is done in Sections 4 and 5. First, in Section 2, we survey previous work on bases, complementarity, measurement, control and the classical-quantum distinction within graphical calculus.

2 Bases, complementarity, measurement, control

We assume that the reader is familiar with the relevant category-theoretic background for the categorical formalization of quantum mechanics, which is surveyed in [9]. We recall some basic concepts from [8,6,4]. All our categories in this paper will be symmetric monoidal \dagger -categories ($\dagger \equiv$ “dagger”), and we will work within

the corresponding graphical calculus [23].

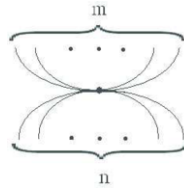
Let (X, δ, ϵ) be a *special commutative \dagger -Frobenius algebra* in a symmetric monoidal \dagger -category \mathbf{C} , or in short, a *classical structure*. Graphically, we depict the monoid comultiplication δ and its unit by ϵ :



As a consequence of the *spider theorem* [18], these classical structures enable intuitive graphical reasoning. This theorem implies that any morphism obtained by means of the monoid multiplication of a classical structure (X, δ, ϵ) , its unit, composition, tensor, dagger and the structural morphisms of symmetric monoidal \dagger -categories only depends on its type:

$$\underbrace{X \otimes \dots \otimes X}_n \rightarrow \underbrace{X \otimes \dots \otimes X}_m.$$

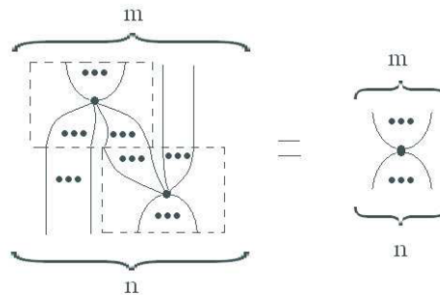
We represent that unique morphism of this type as follows:



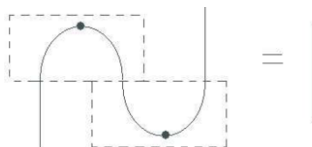
Special cases are:

- $\text{spider}(n = 1, m = 2) = \delta$
- $\text{spider}(n = 1, m = 0) = \epsilon$
- $\text{spider}(n = 1, m = 1) = 1_X$

It follows that these ‘spiders’ compose as follows:



that is, dots corresponding to the same classical structure can be ‘fused’ together. A particular example of this is:



that is, classical structures always carry a (self-dual) \dagger -compact structure [1,22,6]. Hence for each morphism $f : X \rightarrow Y$ between (the objects supporting) two classical structures $(X, \delta_X, \epsilon_X)$ and $(Y, \delta_Y, \epsilon_Y)$ always admits a *transpose* and an *conjugate*, that is, when depicting the dagger of

$$f \equiv \begin{array}{c} | \\ \diagup \text{f} \diagdown \\ | \end{array} \quad \text{as} \quad f^+ \equiv \begin{array}{c} | \\ \diagdown \text{f} \diagup \\ | \end{array}$$

then

$$f^\top \equiv \begin{array}{c} | \\ \text{f} \diagdown \\ | \end{array} := \begin{array}{c} \bullet \\ \text{f} \diagdown \\ | \end{array}$$

and

$$\bar{f} \equiv \begin{array}{c} | \\ \text{f} \diagup \\ | \end{array} := \begin{array}{c} \bullet \\ \text{f} \diagup \\ | \end{array}$$

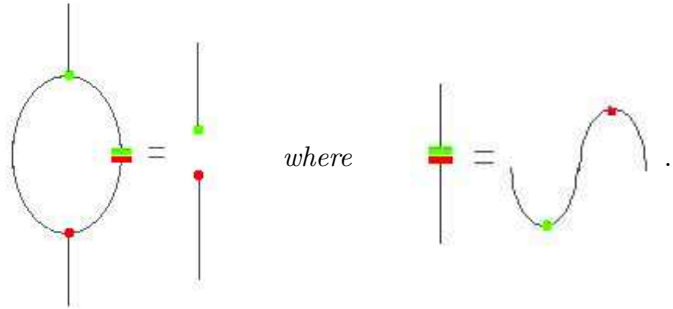
Let **FdHilb** be the symmetric monoidal \dagger -category of finite dimensional Hilbert spaces, linear maps the tensor product, and linear-algebraic adjoints. In this category classical structures *are* precisely orthonormal bases:

Proposition 2.1 [10] *For any orthonormal basis $\{|i\rangle\}$ of a Hilbert space \mathcal{H}*

$$\delta :: |i\rangle \mapsto |ii\rangle \quad \text{and} \quad \epsilon :: |i\rangle \mapsto 1$$

*are the multiplication and the unit of a classical structure in **FdHilb**. Conversely, every classical structure in **FdHilb** arises in this manner.*

Proposition 2.2 [4] *In the light of Proposition 2.1, two classical structures correspond to complementary orthonormal bases if and only if:*

(1) 

In quantum theory bases represent classical data for some observable, hence the

name classical structure. A morphism $f : A \rightarrow B$ is *unitary* iff $f \circ f^\dagger = 1_B$ and $f^\dagger \circ f = 1_A$. Given a classical structure and a unitary morphism U , also

$$(2) \quad \begin{array}{c} \text{Diagram showing a classical structure } U \text{ (represented by a trapezoid) and a unitary morphism } U \text{ (represented by a box). The diagram shows } U \text{ acting on a classical structure, resulting in a unitary morphism } U. \end{array}$$

is a classical structure, where, in the light of Proposition 2.1, U maps the basis of the constructed classical structure on the basis of the given one.

Following [6], $m : X \otimes A \rightarrow B$ represents a *controlled unitary* iff

$$(3) \quad \begin{array}{c} \text{Diagram showing a controlled unitary } m \text{ (represented by a box) acting on a classical structure } X \otimes A \text{ (represented by a trapezoid). The diagram shows } m \text{ acting on } X \otimes A, \text{ resulting in } B. \end{array}$$

Here the X -input takes classical data, i.e. a basis vector $|i\rangle$, and depending on that data a certain unitary $m \circ (|i\rangle \otimes 1_A) : A \rightarrow B$ is performed.⁴

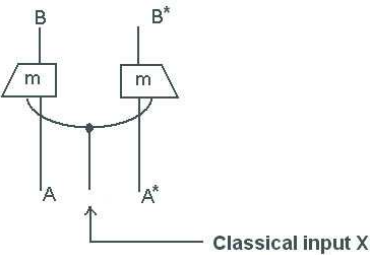
But how do we distinguish classical and quantum wires in the graphical language? Since measurements produce probabilistic outputs we will need to consider probabilistic classical data. Given a basis in a Hilbert space, this can be represented by density matrices which are diagonal. Selinger provided a diagrammatic account on mixed states as completely positive maps in [22], as a categorical construction on the category **FdHilb**. He produced a new category **CPFdHilb** which has the same objects but with has morphisms

$$\begin{array}{c} \text{Diagram showing a morphism } f : A \rightarrow B \text{ (represented by a box) and a morphism } f : A^* \rightarrow B^* \text{ (represented by a box). The diagram shows } f \text{ acting on } A \text{ and } A^*, \text{ resulting in } B \text{ and } B^*. \end{array}$$

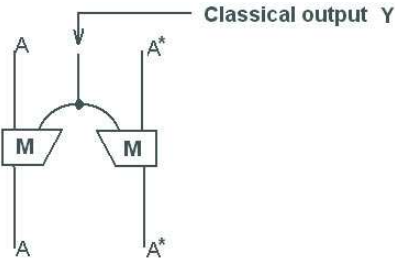
as those of type $A \rightarrow B$, where $f : A \rightarrow B \otimes C$ is any morphism in **FdHilb**, and where the cap-shaped wire comes from the compact structure of **FdHilb**, i.e. $|ij\rangle \mapsto \delta_{ij}$. So any quantum system is in fact represented by two wires. In [6] it was realized that to force classical data to be ‘diagonal in some basis’ it sufficed to pass from the double-wire representation to a single wire by means of a classical structure, e.g. a controlled unitary operation, rather than the morphism m in (3), is in fact a

⁴ The reason for the notation m will become clear below.

morphism:

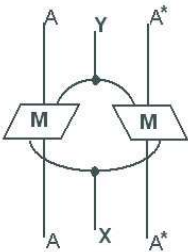


with m as in (3), while a non-destructive measurement would take the form:



where M is subject to certain conditions spelled out in [8]. Given the importance of morphisms satisfying (3) we will continue to refer to these as controlled unitaries (as opposed to controlled unitary ‘operations’).

Definition 2.3 [6] Consider classical structures $(X, \delta_X, \epsilon_X)$ and $(Y, \delta_Y, \epsilon_Y)$ in a symmetric monoidal \dagger -category \mathbf{C} . A *controlled non-destructive measurement* in \mathbf{C} with *control* $(X, \delta_X, \epsilon_X)$ and *outcomes* $(Y, \delta_Y, \epsilon_Y)$ is a morphism:



where M is such that:

(4)

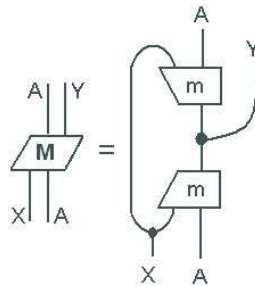
Three equations defining the properties of M :

- Equation 1: A box M with input X and output A is equal to a box M with input X and output A , where the output A is connected to a box M with input A and output Y .
- Equation 2: A box M with input X and output A is equal to a box M with input X and output A , where the output A is connected to a box M with input A and output Y .
- Equation 3: A box M with input X and output A is equal to a box M with input X and output A , where the output A is connected to a box M with input A and output Y .

Similarly, a *controlled destructive measurement* is a morphism

(5) 

which is such that



obeys (4) and hence induces a controlled non-destructive measurement.

Proposition 2.4 [8,6] *For every family of exhaustive projector spectra*

$$\left\{ \{P_i^k : \mathcal{H} \rightarrow \mathcal{H}\}_i \right\}_k,$$

i.e. for all i, j, k we have

$$P_i^k \circ P_j^k = \delta_{ij} P_i^k, \quad P_i^{k\dagger} = P_i^k \quad \text{and} \quad \sum_i P_i^k = 1_{\mathcal{H}},$$

the linear map

$$M := \sum_{i,k} (|i\rangle\langle k|) \otimes P_i^k$$

satisfies (4) and hence defines a controlled non-destructive measurement in $\mathbf{CPFdHilb}$ with as outcomes the classical structure corresponding to orthonormal basis $\{|i\rangle\}_i$ and with as control the classical structure corresponding to orthonormal basis $\{|k\rangle\}_k$. Conversely, every controlled non-destructive measurement in $\mathbf{CPFdHilb}$ arises in this manner.

Proposition 2.5 *The analogous statement to Proposition 2.4 for controlled destructive measurements in $\mathbf{CPFdHilb}$ also holds.*

Proposition 2.6 *If in (5) we take m to be a controlled unitary then we always obtain a controlled destructive measurement.*

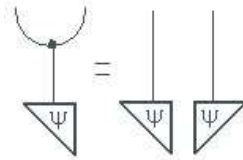
We call these controlled measurements *non-degenerate*, since in $\mathbf{CPFdHilb}$ these exactly correspond with non-degenerate non-destructive measurements.

Here we consider arbitrary collections of measurements. These are not that useful for practical purposes. We now state a similar result for controlled collections of destructive measurements which are pairwise complementary.

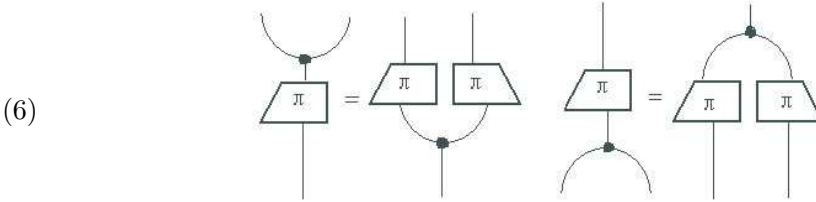
3 Controlled complementary bases

For reasons of clarity we restrict ourselves here to non-destructive measurements, for which there is a direct correspondence with controlled unitaries (cf. Proposition 2.6) and hence also with families of bases.

We recall some more notions from [6] which in part trace back to [3]. A *classical point* for a classical structure is a morphisms $\psi : I \rightarrow A$ such that:



A *permutation* for a classical structure is morphism $\pi : A \rightarrow B$ such that:



This in particular implies that π is self-conjugate.

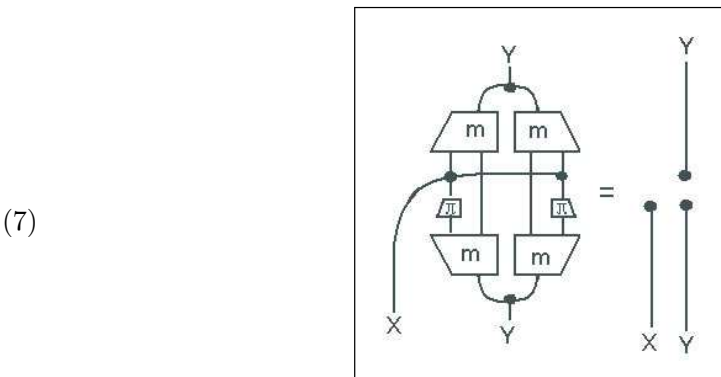
Definition 3.1 A permutation is *fixed-point free* iff for any classical point ψ of the corresponding classical structure we have that $\pi \circ \psi \neq \psi$.

Proposition 3.2 In **FdHilb** fixed-point free permutations are linear maps

$$|i\rangle \mapsto |\pi(i)\rangle$$

where $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ is an ordinary fixed-point free permutation.

Definition 3.3 A *controlled complementary measurement* is a morphism (5) with m a controlled unitary such that:



for all fixed-point free permutations π . In that case we call m *controlled complementary unitaries*, and the corresponding controlled classical structure (cf. (2)) *complementary classical structures*, or shorter, *complementary bases*.

The following theorem justifies our terminology.

Theorem 3.4 For complementary bases $\{\{|i\rangle^k\}_i\}_k$, i.e.

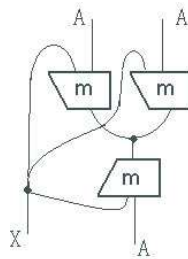
$${}^k\langle i|j\rangle^l = \begin{cases} \delta_{ij} & \text{for } k = l \\ \frac{1}{\sqrt{\dim(\mathcal{H})}} & \text{for } k \neq l \end{cases}$$

the linear map:

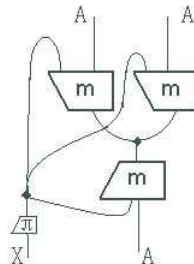
$$m := \sum_{i,k} (|i\rangle\langle k|) \otimes |i\rangle^k$$

satisfies (7) for all fixed-point free permutations π (and hence defines a controlled complementary measurement in **CPFdHilb**). Conversely, all controlled complementary unitaries in **CPFdHilb** arise in this manner.

Proof. The crux to the proof is the following. Given controlled unitaries m , the corresponding bases (cf. (2)) are:

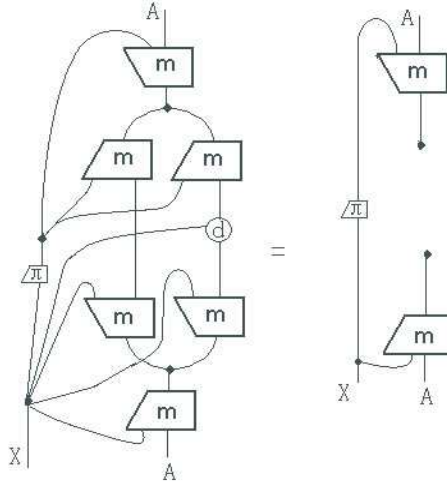


For a given value of the control variable, that is, the choice of a basis, we obtain another basis for the same value as follows:

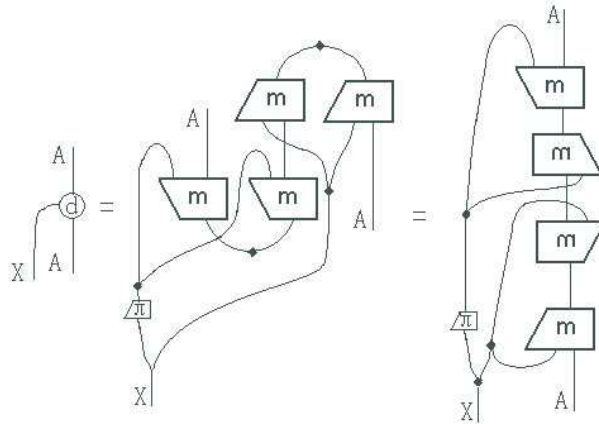


By ranging over all fixed-point free permutations and all values of the control variable we obtain all possible pairs of bases. To assert complementarity of all pairs we

substitute all of these in (1) which results in:



where



Using (3) and canceling the outer controlled unitaries in both pictures we indeed obtain (7). \square

Note that the crux of the proof does not rely on the concrete Hilbert space structure but on the abstract analysis of complementarity in [4]. Hence our abstract definition of controlled complementary unitaries naturally extends to a broad class of potential models.

4 Graphic calculus for BB84 and Ekert 91

The procedure of BB84 is as follows [2]:

- (i) Alice chooses two random bit string $\alpha = \alpha_1 \dots \alpha_{4n}$ and $a = a_1 \dots a_{4n}$.
- (ii) Alice *encodes* each bit α_i as qubit in a manner depending on a_i . A bit $\alpha_i = 0$ is encoded as $q_i = |0\rangle$ if $a_i = 0$ and as $q_i = |+\rangle$ if $a_i = 1$, and a bit $\alpha_i = 1$ is encoded as $q_i = |1\rangle$ if $a_i = 0$ and as $q_i = |-\rangle$ if $a_i = 1$.

- (iii) Alice transfers the quantum bits via a quantum channel to Bob.
- (iv) Bob chooses random bit string $b = b_1 \dots b_{4n}$ and measures each qubit q_i in the Z -basis if $b_i = 0$ and in the X -basis if $b_i = 1$, yielding $\beta = \beta_1 \dots \beta_{4n}$.
- (v) Bob sends b to Alice via a conventional channel.
- (vi) Alice sends $a \oplus b = a_1 \oplus b_1 \dots a_{4n} \oplus b_{4n}$ to Bob via a conventional channel.
- (vii) Alice (resp. Bob) only retain those bits α_i in α (resp. β_i in β) for which $a_i \oplus b_i = 0$ and discard the others.

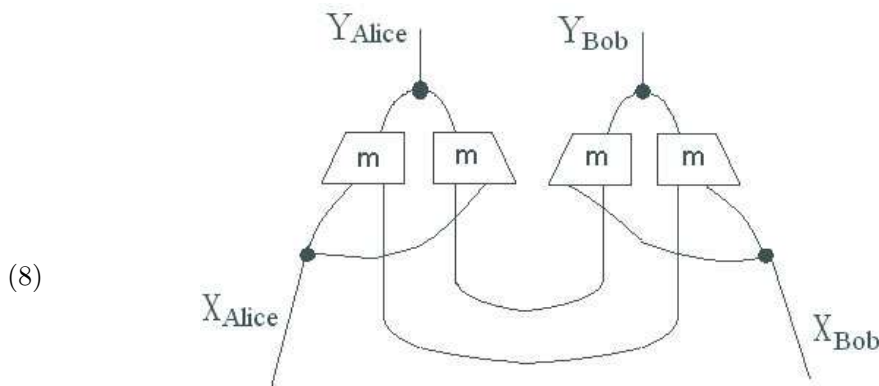
In the absence of an attack both resulting strings, which have an average length of $2n$, coincide. Denote it as $\omega = \omega_1 \dots \omega_n$. Next Alice and Bob wish to verify whether no attack by Eve has taken place.

- (viii) Alice and Bob agree of a subset of n bits of their respective strings ω^{Alice} and ω^{Beta} and compare their values for these.
- (ix) If all bits of ω^{Alice} and ω^{Beta} match Alice and Bob use the remaining string $\tilde{\omega}$, which has an average length of n , as a private key for purposes of conventional cryptography.

The procedure of Ekert91 is as analogous; Alice and Bob share a Bell state,⁵ then both perform (iv), and next (v)–(ix).

We can now use the results of the previous section to translate these protocols into graphical language. Note that (ii) can be realized by means of a a -controlled unitary which applies the identity for $a_i = 0$ and the Hadamard gate for $a_i = 1$. By Proposition 2.6 it then follows that both protocols are highly related. We obtain for the procedures till (vii):

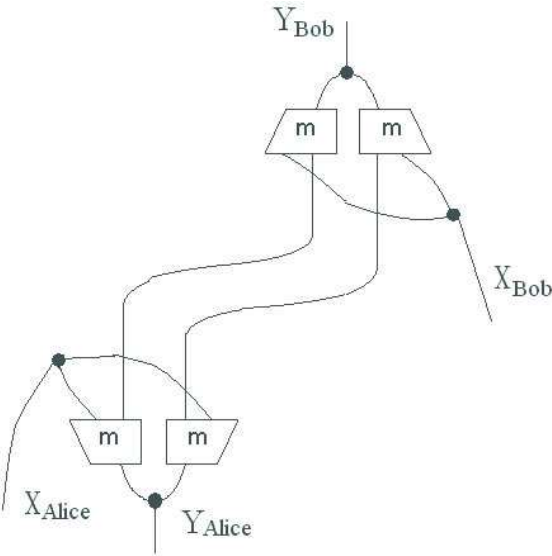
Ekert91:



⁵ Establishing that this is indeed a Bell-state is part of the protocol.

BB84:

(9)



where $X_{Alice} = X_{Bob} = Y_{Alice} = Y_{Bob} = A = \mathbb{C}^{\oplus 2}$ and

$$m : X_- \otimes A \rightarrow Y_- :: |00\rangle \mapsto |0\rangle, |01\rangle \mapsto |1\rangle, |1+\rangle \mapsto |0\rangle, |1-\rangle \mapsto |1\rangle,$$

that is, as a matrix,

$$(I \ H) = \begin{pmatrix} 1 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 1 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

where I is the 2×2 identity matrix and H is the Hadamard gate.

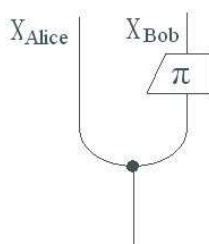
The pictures expose that both protocols are interconvertible by mere transposition. Hence whatever we prove about one can be immediately translated to the other. Below we choose to consider the Ekert 91 protocol.

We now wish to show that in the graphical language the correctness of these protocols, that is, when the control inputs of Alice and Bob coincide, the information from Alice can be fully transferred to Bob, but when the control inputs of Alice and Bob are different, there is no information flow from Alice to Bob. In terms of the topology of pictures the first case means that Alice and Bob are ‘connected’ (by an identity) while the second case means that Alice and Bob are ‘disconnected’.

We can assert that the control inputs coincide as:

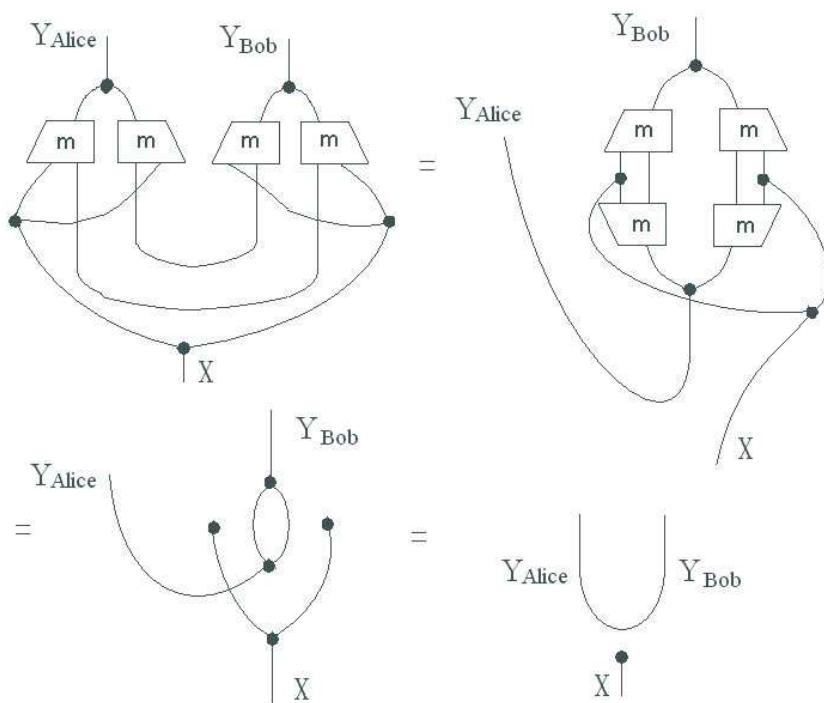


and that they do not coincide as:

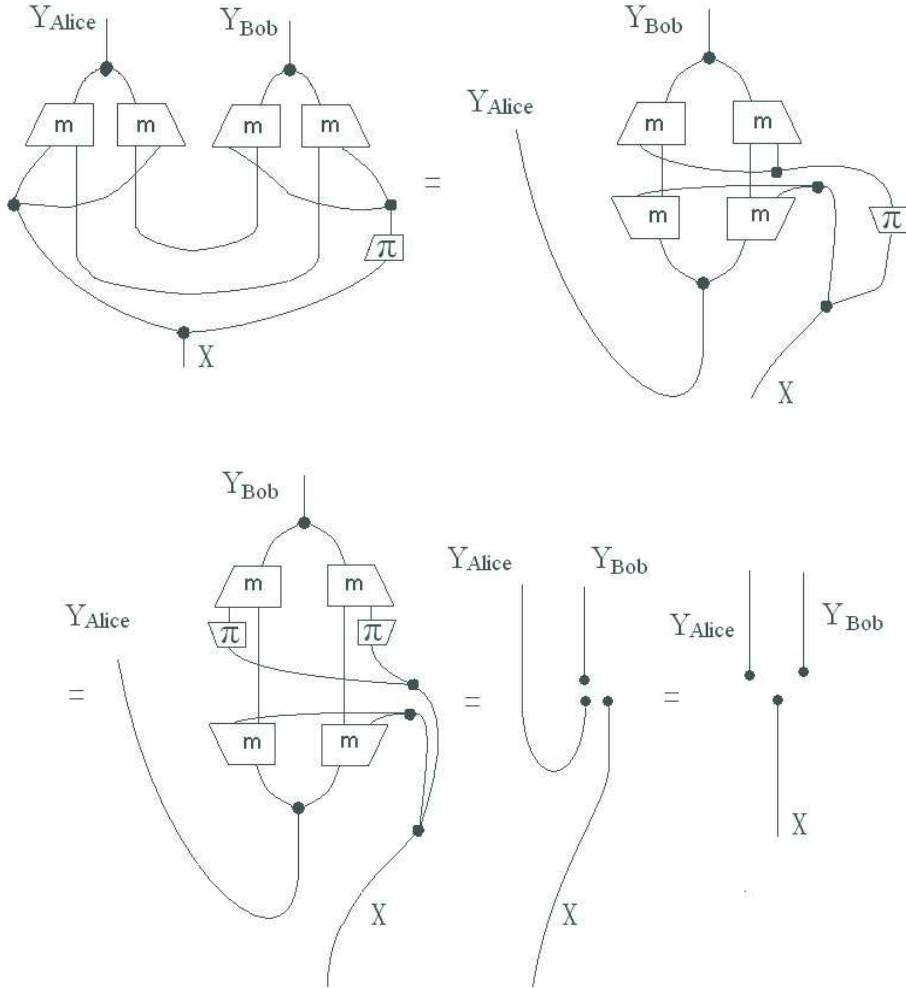


where π is the only fixed-point free permutation of $\{0, 1\}$, i.e. NOT.

Let $(X, \delta_X, \epsilon_X)$ and $(Y, \delta_Y, \epsilon_Y)$ be classical structures in *any* symmetric monoidal \dagger -category \mathbf{C} , let $m : X \otimes A \rightarrow Y$ be *any* controlled unitaries, and let $\pi : X \rightarrow X$ be *any* fixed-point free permutation. Then:



where we used (3). If m is moreover complementary then:



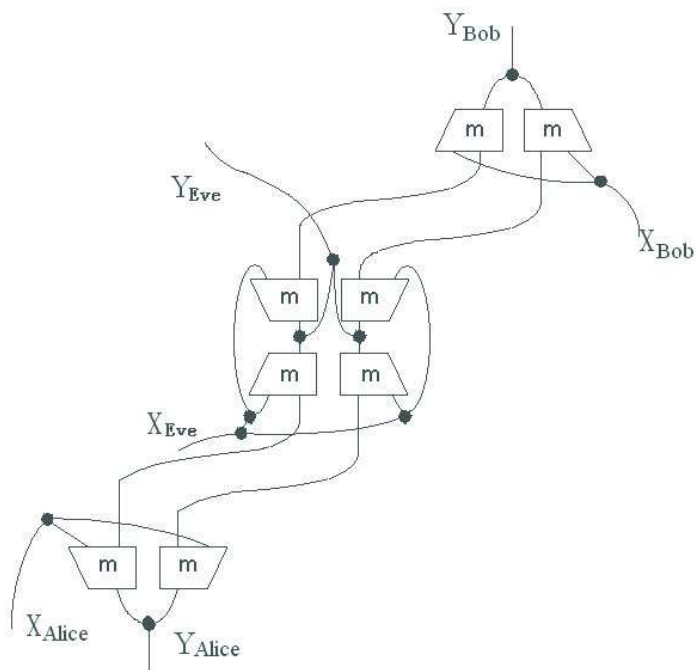
where we used (7) and (6). The first case of coinciding choices has already previously been considered by Heunen in [15] §3.3. Our contribution here is the case that the chosen bases are complementary.

5 An intercept-resend attack on BB84

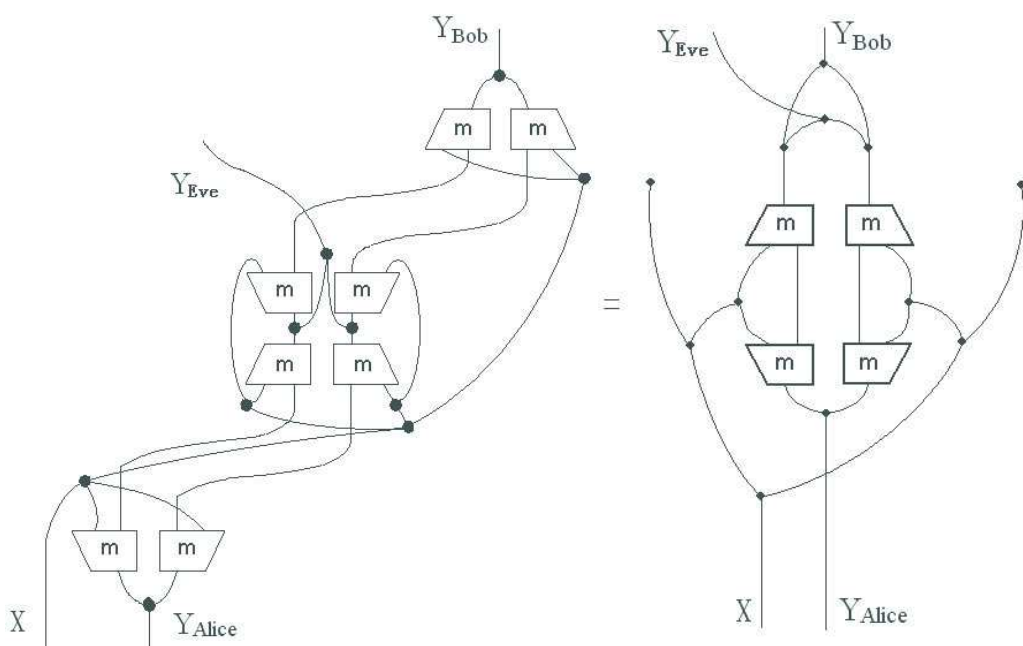
To illustrate the security of BB84, let us consider the simple example of an intercept-resend attack by an eavesdropper Eve, who measures each qubit (quickly enough so that Bob cannot detect interference) sent by Alice in a randomly chosen basis and then resends the resulting state to Bob. Since the two bases are chosen randomly by each party, such an intercept-resend attack will give a bit error rate of $0.5 \times 0.5 = 0.25$, which is readily detectable by Alice and Bob in part (viii) of the BB84 protocol.

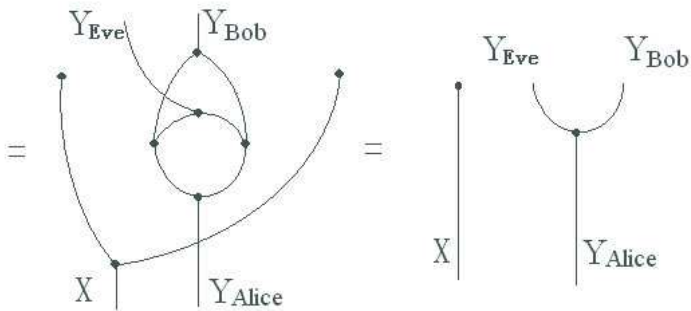
Intercept-resend attack on BB84:

(10)

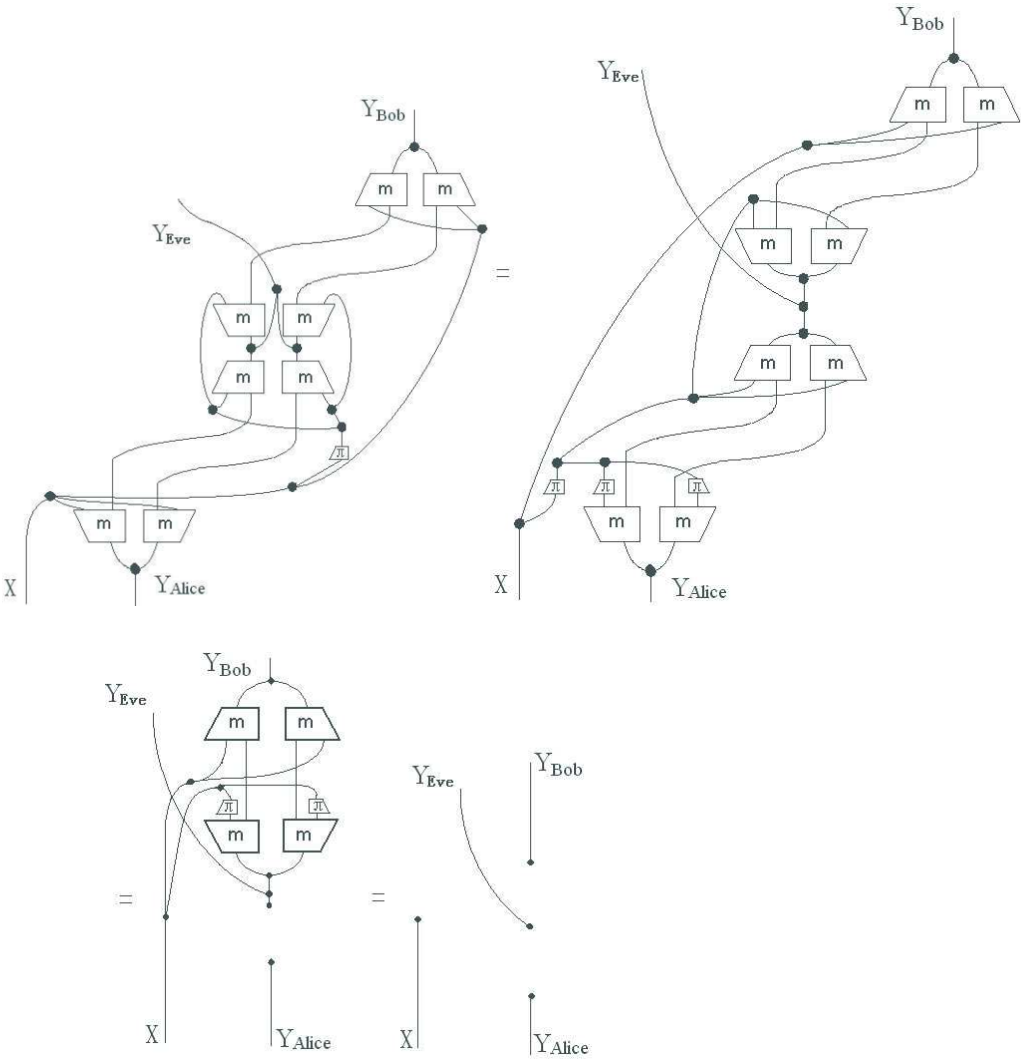


Now again considering a general symmetric monoidal \dagger -category, any pair of classical structures therein, any corresponding controlled complementary unitaries, and any fixed-point free permutation, then:





and:

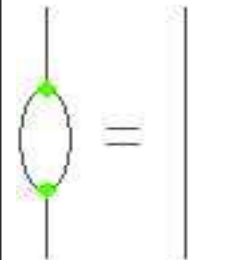
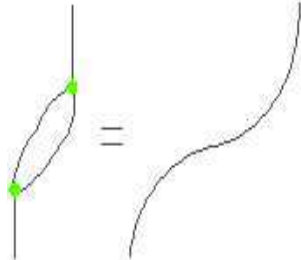
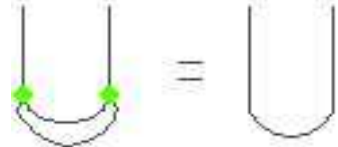
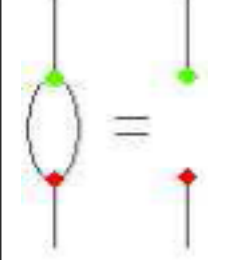
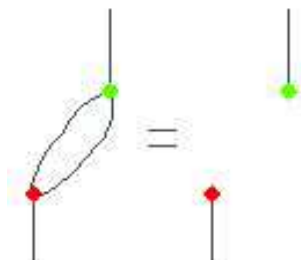
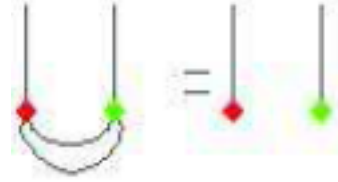


6 Conclusion

We provided a graphical axiomatization of the main quantum key distribution protocols which enabled to very easily prove their correctness as well as their properties in case of an attack. In fact, in doing, due to the abstraction level of our approach, we proved this also for a far more general class of quantum protocols, and also a far more general class of mathematical models.

Key was the axiomatization of controlled complementary unitaries. These obviously have many important applications and also are of foundational importance. Hence we expect many more results to emerge from ours.

A remarkable observation was that the topology of the diagrams expressing ‘the same’ (= specialness of the Frobenius structure) and ‘complementary’ for bases directly translates into the cases ‘same choice’ and ‘different (complementary) choice’ for Alice and Bob in quantum key distribution:

| | axiom | BB84 | Ekert 91 |
|-------|---|---|--|
| same: |  |  |  |
| comp: |  |  |  |

This reveals the crucial role played by the ‘one wire vs. two wires’ manner of distinguishing ‘classical vs. quantum’. It enables using (7) of Definition 3.3 to show correctness in the case of different choices of measurement by Alice and Bob of the quantum key distribution protocols. In turns, the ‘one wire vs. two wires’ in equation (7) is a direct consequence of the ‘Hopf-law’ (1) which asserts complementarity. This points at a new structural connection between the classical-quantum distinction (i.e. decoherence) and complementarity.

One technical issue is that our abstract definition of fixed-point free, while perfectly adequate for our purposes here, may not lift to other models where classical structures may have too few classical points, e.g. the category of finite sets and relations **FRel**. Since the classical structures in **FRel** are meanwhile well understood [5,20,13], and have proven to far more richer than expected, it would be worth to

also study cryptographic phenomena in this realm. One possible alternative account would be to ask for the permutation to have a zero trace, which involves assuming that there is a zero scalar.

A different issue, already considered by Heunen in [14], is an explicit account on unbounded bit strings, which could be blended in here.

References

- [1] S. Abramsky and B. Coecke. *A categorical semantics of quantum protocols*. In: Proceedings of 19th IEEE conference on Logic in Computer Science, pages 415–425. IEEE Press, 2004. arXiv:quant-ph/0402130. Revised and extended version: arXiv:0808.1023
- [2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, 1984. IEEE, New York.
- [3] A. Carboni and R. F. C. Walters *Cartesian bicategories I*. Journal of Pure and Applied Algebra **49**, 11–32, 1987.
- [4] B. Coecke and R. Duncan. *Interacting quantum observables*. In: Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP), pp. 298–310, Lecture Notes in Computer Science 5126, Springer-Verlag, 2008. Revised and extended version: arXiv:0906.4725
- [5] B. Coecke and B. Edwards. *Toy quantum categories*. Electronic Notes in Theoretical Computer Science, to appear. arXiv:0808.1037
- [6] B. Coecke, E. O. Paquette and D. Pavlovic. *Classical and quantum structuralism*. In: Semantic Techniques for Quantum Computation, I. Mackie and S. Gay (eds), pages 29–69, Cambridge University Press. arXiv:0904.1997
- [7] B. Coecke, E. O. Paquette and S. Perdrix. *Bases in diagrammatic quantum protocols*. Electronic Notes in Theoretical Computer Science **218**, 131–152, 2008. arXiv:0808.1037
- [8] B. Coecke and D. Pavlovic. *Quantum measurements without sums*. In: Mathematics of Quantum Computing and Technology, G. Chen, L. Kauffman and S. Lomonaco (eds), pages 567–604. Taylor and Francis, 2007. arXiv:quant-ph/0608035
- [9] B. Coecke and E. O. Paquette. *Categories for the practicing physicist*. In: New Structures for Physics, B. Coecke (ed), pages 167–271. Lecture Notes in Physics, Springer-Verlag, 2010. arXiv:0905.3010
- [10] B. Coecke, D. Pavlovic and J. Vicary. *A new description of orthogonal bases*. arXiv:0810.0812
- [11] R. Duncan and S. Perdrix. *Graph states and the necessity of Euler decomposition*. In: Proceedings of Computability in Europe: Mathematical Theory and Computational Practice (CiE’09), pages 167–177. Lecture Notes in Computer Science 5635, Springer-Verlag, 2009. arXiv:0902.0500
- [12] A. Ekert. *Quantum cryptography based on Bell’s theorem*. Physical Review Letters **67**, pp. 661–663, 1991.
- [13] J. Evans, R. Duncan, A. Lang and P. Panangaden. *Classifying all mutually unbiased bases in Rel*. arXiv:0909.4453
- [14] C. Heunen (2008) *Compactly accessible categories and quantum key distribution*. Logical Methods in Computer Science **4**, issue 4, paper 9. arXiv:0811.2113
- [15] C. Heunen (2009) *Categorical Quantum Models and Logics*. Ph.D. Thesis, Radboud Universiteit Nijmegen.
- [16] A. Joyal and R. Street. *The Geometry of tensor calculus I*. Advances in Mathematics **88**, 55–112, 1991.
- [17] G. M. Kelly and M. L. Laplaza. *Coherence for compact closed categories*. Journal of Pure and Applied Algebra **19**, 193–213, 1980.
- [18] S. Lack. *Composing PROPs*. Theory and Applications of Categories **13**, 147–163, 2004.
- [19] G. Lowe. *An attack on the Needham-Schroeder public key authentication protocol*. Information Processing Letters **56**, 131–136, 1995.
- [20] D. Pavlovic. *Quantum and classical structures in nondeterministic computation*. Lecture Notes in Computer Science **5494**, page 143–157, Springer, 2009. arXiv:0812.2266

- [21] R. Penrose. *Applications of negative dimensional tensors*. In: *Combinatorial Mathematics and its Applications*, D. Welsh (Ed), pages 221–244. Academic Press, 1971.
- [22] P. Selinger (2007) *Dagger compact closed categories and completely positive maps*. *Electronic Notes in Theoretical Computer Science* **170**, 139–163.
- [23] P. Selinger. *A survey of graphical languages for monoidal categories*. In: *New Structures for Physics*, B. Coecke (ed), pages 275–337. Lecture Notes in Physics, Springer-Verlag, 2010. arXiv:0908.3347