Picture-perfect Quantum Key Distribution

(Extended Abstract)

Aleks Kissinger [†]
Radboud University Nijmegen
aleks@cs.ru.nl

Sean Tull [*]
University of Oxford
sean.tull@cs.ox.ac.uk

Bas Westerbaan [†]
Radboud University Nijmegen
bas@westerbaan.name

A full version of this article will shortly be submitted to Quantum. *Preprint:* arXiv:1704.08668.

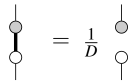
We provide a new way to bound the security of quantum key distribution using only the diagrammatic behavior of complementary observables and essential uniqueness of purification for quantum channels. We begin by demonstrating a proof in the simplest case, where the eavesdropper doesn't noticeably disturb the channel at all and has no quantum memory. We then show how this case extends with almost no effort to account for quantum memory and noise.

Quantum Key Distribution is an unauthenticated key agreement protocol allowing two agents, Alice and Bob, with means of exchanging qubits, to securely agree on a secret key [2, 12, 7]. Following the original 'BB84' proposal by Bennet and Brassard [2], there have been several variations, notably the 'E91' protocol [7]. Not everyone was satisfied by the original proof of security of BB84, and numerous authors presented more meticulous [9] or 'simple' [11] proofs. This did not settle the matter: there have been many subsequent publications on the security of BB84 and its variants [10].

In the full version of this article, we derive a bound on the security of BB84. The proof is short enough to be sketched here, and simple enough to be given entirely diagrammatically, using the graphical approach to quantum information [6] growing out of the field of categorical quantum mechanics [1]. Our proof relies on the graphical expression of *complementary* quantum measurements [4] and the ability to *purify* mixed quantum processes in an 'essentially unique' way. The latter has already been used to derive many quantum-like features by Chiribella et al. in the setting of general probabilistic theories [3].

Let us briefly recall the BB84 protocol. Alice wishes to securely establish a secret key with Bob. They share a Hilbert space H of dimension 2, fixing in advance a pair of orthonormal bases which are mutually unbiased, i.e. complementary. Alice generates several random bits and encodes each as a qubit randomly in one of the two bases, transmitting it to Bob, who measures it randomly in one of the bases. When their choices match, the bit is transmitted perfectly, and otherwise since the bases are unbiased, no information is conveyed. Afterwards, Alice and Bob can publicly announce their basis choices (since this information is totally random), knowing that whenever they agreed, a bit should have been transmitted. They randomly pick a subset of these bits, checking that their values agree, and if so use the remaining bits as a secret key.

Graphically, we represent the protocol with the help of *spiders*. Each orthonormal basis (ONB) of a finite-dimensional Hilbert space H corresponds uniquely to a family of linear maps called spiders. Hence, two ONBs $\{|z_i\rangle\}$ and $\{|x_i\rangle\}$ can be represented as two different families of spiders, depicted as white and gray dots, respectively. These ONBs are mutually unbiased whenever their spiders satisfy an equation known as *complementarity* [5]. This equation has several equivalent forms, the most operationally striking of which is the following, in terms of the *encoding* and *measuring* processes associated with a spider:



(1)

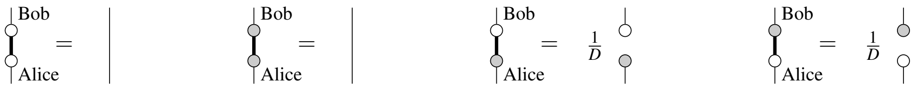
[*] Supported by EPSRC Studentship OUCL/2014/SET.

[†] Supported by the European Research Council under grant agreement 320571.

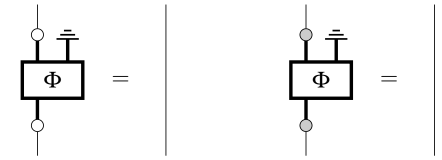
Submitted to:
QPL 2017

Thick wires represent quantum systems $\mathscr{B}(H)$, whereas thin wires represent classical systems H, where we consider vectors in H as probability distributions. Intuitively, equation (1) means that if we encode a classical value as a quantum system using the ONB $\{|z_i\rangle\}$ of quantum states then measure using $\{|x_i\rangle\}$, the measurement result has no correlation with the original value.

Using (1), we see the four different possibilities of Alice and Bob choosing the basis $\{|z_i\rangle\}$ or $\{|x_i\rangle\}$ in QKD result in the following outcomes, as expected:

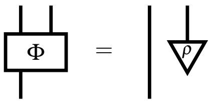


Now suppose that some eavesdropper, Eve, is intercepting the transmitted qubits and attempts to learn about them, by applying some quantum channel $\Phi\colon \mathscr{B}(H) \to \mathscr{B}(H \otimes E)$ to each. To remain completely undetected, the partial trace of Φ on H must not affect Bob's outcome whenever his basis agrees with Alice's. We depict the trace with the 'ground' symbol, and this condition as:

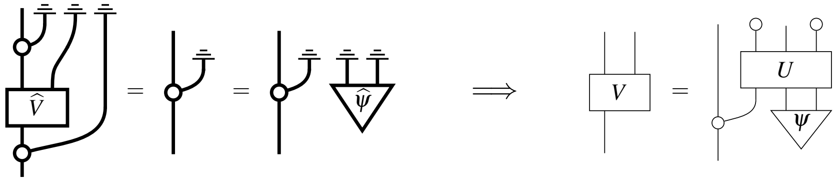


(2)

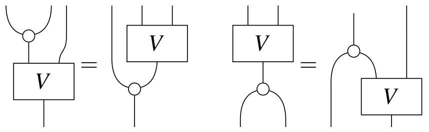
Theorem. In this situation Eve's channel separates. That is, there is a state ρ of $\mathscr{B}(E)$ such that:



Proof. Since Eve's system is arbitrarily large, by applying purification we can assume that Φ is pure. That is, there exists a linear map V such that $\Phi(\rho) = \widehat{V}(\rho) := V\rho V^\dagger$. In what follows we depict such maps with thin wires. The first equation in (2) implies the existance of two distinct purifications of the same quantum channel. Hence, by essential uniqueness, these purifications are related by a unitary U:

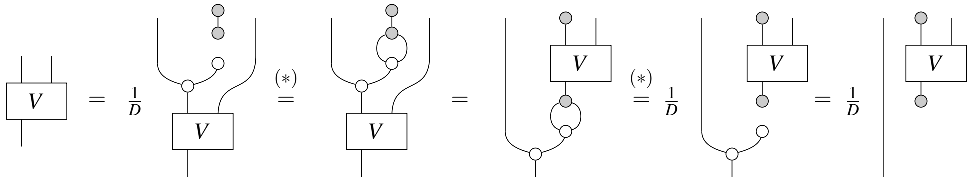


where ψ is any pure state of $E \otimes H$. It follows from graphical spider rules that:



(3)

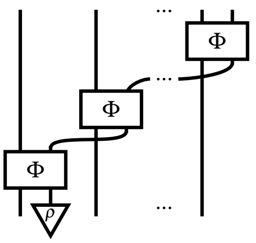
and the same equations hold for the gray spider. V (and hence Φ) then separates as follows:



where $(*)$ uses an equivalent version of the complementarity equation (1). □

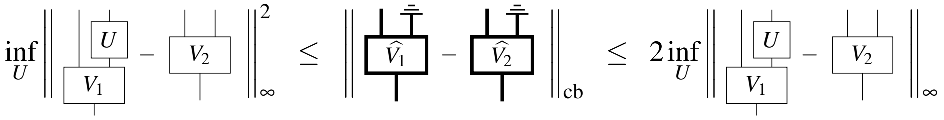
The simplicity of the graphical approach makes clear several immediate generalizations. Most simply, the same proof applies regardless of the dimension D of Alice and Bob's Hilbert space — all that is necessary is a pair of complementary bases.

More significantly, the same proof extends to the case in which Eve has access to a *quantum memory* which she may use to store information between transmissions. In this case, the memory is read through an extra input in her channel Φ, which is initially prepared in some state ρ. Eve's overall procedure, after n transmissions between Alice and Bob, amounts to the channel:

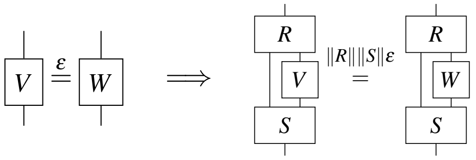


For Eve to remain completely undetected amounts to the analogous equation to (2) for each matching input and output of the above, after tracing out all others. Starting from the first input, our previous results shows that $\Phi \circ (\mathrm{id} \otimes \rho)$ separates, and then inductively that Eve's whole procedure does.

Though our proofs so far have been interesting, to fully establish security of the protocol requires us to demonstrate noise tolerance. After all, it could be the case that Eve can extract a lot of information about the transmitted bits by only disturbing them slightly. In fact, this worry is unjustified, and the same diagrammatic proof establishes a noise tolerant result as follows. The corner-stone is the continuous version of the essential uniqueness of purifications due to Kretschmann, Schlingemann and Werner [8], which states that for any pure maps $V_1, V_2 \colon H \to K \otimes L$ we have:



where the infima are taken over all unitaries U on L. Here $\|-\|_\infty$ is the operator-norm while $\|-\|_{\mathrm{cb}}$ denotes the *completely bounded norm* (cb-norm) on super-operators. Write $V \overset{\varepsilon}{=} V'$ as shorthand for $\|V - V'\|_\infty \leq \varepsilon$. Then using this result along with the following basic property of the operator norm:



(4)

we can systematically transform the earlier diagrammatic proof to a noise-tolerant version, just by decorating equations with ε's.

Theorem. There is a constant N, depending only on the dimension of Alice and Bob's system, such that whenever (2) holds up to ε in the cb-norm, Ψ is within $N\sqrt{\varepsilon}$ of $\mathrm{id} \otimes \rho$ in the cb-norm, for some state ρ of $\mathscr{B}(E)$.

So far in the literature, diagrammatic methods have mainly been used for exact reasoning about quantum processes. The proof of our final result, based on the rule (4), suggests its use in other noise tolerant investigations of quantum protocols, and we call this technique *ε-bounded diagrammatic reasoning*. It promises to provide a useful tool for the future investigation of further quantum protocols, combining the intuitive high-level power of diagrammatic approach with a rigorous treatment of noise tolerance.

References

[1] S. Abramsky & B. Coecke (2004): *A Categorical Semantics of Quantum Protocols*. In: *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science (LICS)*, IEEE Computer Society, pp. 415–425, DOI: 10.1109/lics.2004.1319636. arXiv:quant-ph/0402130.

[2] C. H. Bennett & G. Brassard (1984): *Quantum Cryptography: Public Key Distribution and Coin Tossing*. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, IEEE, pp. 175–179, DOI: 10.1016/j.tcs.2014.05.025.

[3] G. Chiribella, G. M. D'Ariano & P. Perinotti (2010): *Probabilistic theories with purification*. *Physical Review A* 81(6), p. 062348, DOI: 10.1103/physreva.81.062348.

[4] B. Coecke & R. Duncan (2008): *Interacting quantum observables*. In: *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP)*, Lecture Notes in Computer Science, DOI: 10.1007/978-3-540-70583-3_25.

[5] B. Coecke & R. Duncan (2011): *Interacting quantum observables: categorical algebra and diagrammatics*. *New Journal of Physics* 13, p. 043016. arXiv:quant-ph/09064725.

[6] B. Coecke & A. Kissinger (2014): *Picturing Quantum Processes*. Cambridge University Press, DOI: 10.1017/9781316219317.

[7] A. K. Ekert (1991): *Quantum cryptography based on Bell's theorem*. *Physical Review Letters* 67(6), pp. 661–663, DOI: 10.1103/physrevlett.67.661.

[8] D. Kretschmann, D. Schlingemann & R. F. Werner (2008): *The information-disturbance tradeoff and the continuity of Stinespring's representation*. *IEEE transactions on information theory* 54(4), pp. 1708–1717, DOI: 10.1109/tit.2008.917696.

[9] D. Mayers (2001): *Unconditional security in quantum cryptography*. *Journal of the ACM (JACM)* 48(3), pp. 351–406, DOI: 10.1145/382780.382781.

[10] R. Renner (2008): *Security of quantum key distribution*. *International Journal of Quantum Information* 6(01), pp. 1–127, DOI: 10.1142/S0219749908003256.

[11] P. W. Shor & J. Preskill (2000): *Simple proof of security of the BB84 quantum key distribution protocol*. *Physical review letters* 85(2), p. 441, DOI: 10.1103/physrevlett.85.441.

[12] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy & H. Zbinden (2002): *Quantum key distribution over 67 km with a plug&play system*. *New Journal of Physics* 4(1), p. 41, DOI: 10.1088/1367-2630/4/1/341.