EINDHOVEN UNIVERSITY OF TECHNOLOGY

Diagrammatic security proof for 8-state encoding

Citation for published version (APA):
Skoric, B., & Wolffs, Z. (2021). Diagrammatic security proof for 8-state encoding. *arXiv*.

Document status and date:
Gepubliceerd: 02/03/2021

Please check the document version of this publication:

• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

Download date: 13. Jun. 2021

arXiv:2103.01936v1 [quant-ph] 2 Mar 2021

Diagrammatic security proof for 8-state encoding

Boris Škorić and Zef Wolffs

Abstract

Dirac notation is the most common way to describe quantum states and operations on states. It is very convenient and allows for quick visual distinction between vectors, scalars and operators. For quantum processes that involve interactions of multiple systems an even better visualisation has been proposed by Coecke and Kissinger, in the form of a diagrammatic formalism [3]. Their notation expresses formulas in the form of diagrams, somewhat similar to Feynman diagrams, and is more general than the circuit notation for quantum computing.

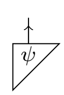
This document consists of two parts. (1) We give a brief summary of the diagrammatic notation of quantum processes, tailored to readers who already know quantum physics and are not interested in general process theory. For this audience our summary is less daunting than the encyclopaedic book by Coecke and Kissinger [3], and on the other hand more accessible than the ultra-compact introduction of [5]. We deviate a somewhat from [3, 5] in that we do not assume basis states to equal their own complex conjugate; this means that we do not use symmetric notation for basis states, and it leads us to explicitly show arrows on wires where they are usually omitted.

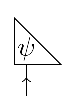
(2) We extend the work of Kissinger, Tull and Westerbaan [5] which gives a diagrammatic security proof for BB84 and 6-state Quantum Key Distribution. Their proof is based on a sequence of diagrammatic manipulations that works when the bases used in the protocol are mutually unbiased. We extend this result to 8-state encoding, which has been proposed as a tool in quantum key recycling protocols [8, 6], and which does *not* have mutually unbiased bases.

1 Pure states and linear operators

In the diagrammatic notation of Coecke and Kissinger, time flows from the bottom to the top, just like in Feynman diagrams. Wires represent states. Boxes of various shapes represent operations. Hermitian conjugation (†) corresponds to vertical flipping. Complex conjugation (c.c.) is horizontal flipping. Taking the transpose is a 180° rotation.

Pure states. The preparation of a pure state $|\psi\rangle$ is depicted as a triangle with a thin directed wire departing from it upwards. The corresponding bra $|\psi\rangle^\dagger = \langle\psi|$, i.e. taking the inner product with ψ, is depicted as a thin directed wire terminating in the vertically flipped triangle. The arrow points towards the bra.

$|\psi\rangle \quad \equiv$ 

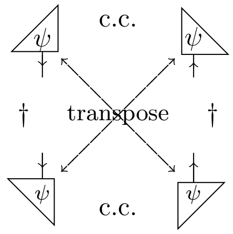
$\langle\psi| \quad \equiv$ 

(1)

The picture below shows $|\psi\rangle$, $\langle\psi|$, $|\psi\rangle^*$ and $\langle\psi|^*$. Note that the wire connected to $|\psi\rangle^*$ and $\langle\psi|^*$ has

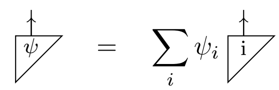
This manuscript is based on Zef Wolffs' bachelor thesis [9].

a *downward* arrow.



(2)

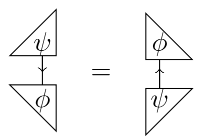
Wires are sometimes labeled with the Hilbert space in which the state lives. Basis states $|i\rangle$ in some orthonormal basis are often represented as a left-right symmetric shape, since their vector representation is typically real-valued. We will depart from this convention because we will be working with a set of bases that does not allow for such simultaneous real-valued representation. We depict the decomposition $|\psi\rangle = \sum_i \psi_i |i\rangle$ as



(3)

Note that a diagram may contain summations and scalar multiplications. A different choice of basis is indicated as a different shading or colour of the basis triangles. The 'standard' basis is white.

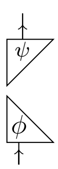
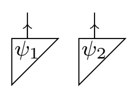
Inner product. The formula $\langle\psi|\phi\rangle^* = \langle\phi|\psi\rangle$ is depicted as



(4)

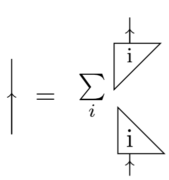
Rotation of a diagram that yields a scalar has no effect on the numerical outcome.

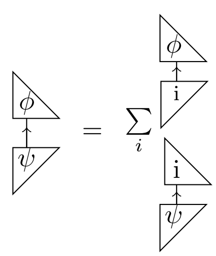
Tensor product. When parts of a diagram are not connected, this indicates that the tensor product is taken. It does not matter how these parts are arranged with respect to each other, e.g. vertically separated or horizontally. This means that *disconnected parts in a diagram may be freely moved around.*

 $\equiv |\psi\rangle \otimes \langle\phi| = |\psi\rangle\langle\phi|$  $\equiv \quad |\psi_1\rangle \otimes |\psi_2\rangle$ (5)

Two parallel wires, one of which represents the identity on Hilbert space $\mathcal{H}_1$ and the other on $\mathcal{H}_2$, may be drawn as a single wire for the tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$.

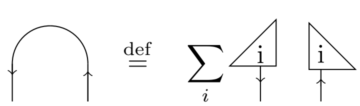
Wires. A wire represents the identity map. The diagrams below depict the spectral decomposition of the identity, $\mathbf{1} = \sum_i |i\rangle\langle i|$, and the formula $\langle\phi|\psi\rangle = \sum_i \langle\phi|i\rangle\langle i|\psi\rangle = \sum_i \phi_i^* \psi_i$.





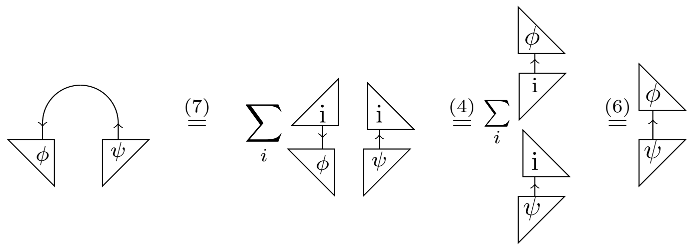
(6)

A bent around wire has the following definition,



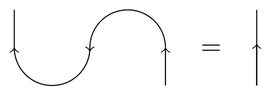
(7)

This definition leads to a very handy visualisation of the formula $\langle\phi|\psi\rangle = \sum_i \langle i|\phi\rangle^* \langle i|\psi\rangle$ as a bent-around version of (6),



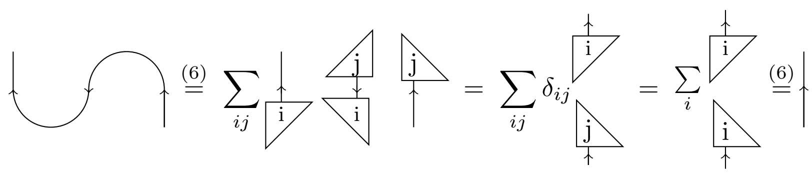
(8)

More generally, it was shown in [3] that wires can be bent in any way without affecting the numerical outcome of a diagram. This goes by the name *yanking equations*. For example, the S-shape bend below is equivalent to a straight wire,



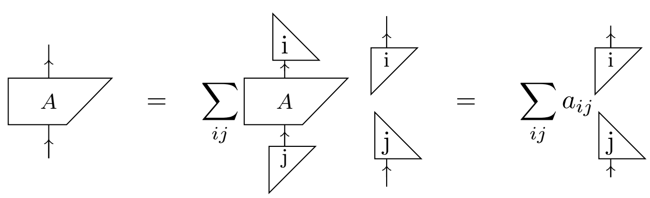
(9)

This is proven diagrammatically as follows.



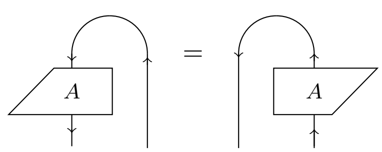
(10)

Linear maps. A linear map $A = \sum_{ij} \langle i|A|j\rangle\ |i\rangle\langle j| = \sum_{ij} a_{ij} |i\rangle\langle j|$ is depicted as



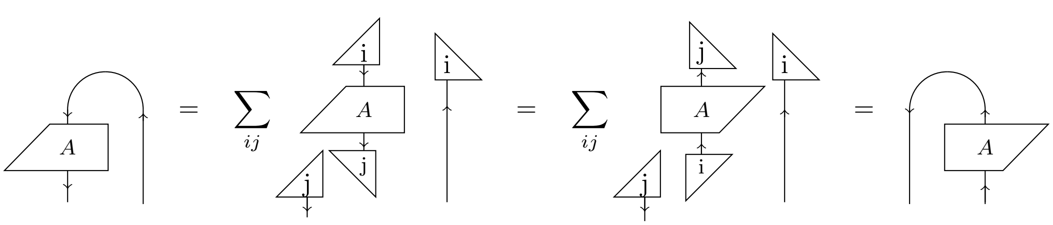
(11)

where the input space and output space do not have to be the same. The incoming and outgoing wire in the diagram above may stand for multiple wires. Note that the shape of the A-box is asymmetric, so that vertical and horizontal flips are easily recognised visually.
A linear map can be moved along a wire, as long as it is rotated along with the bends.



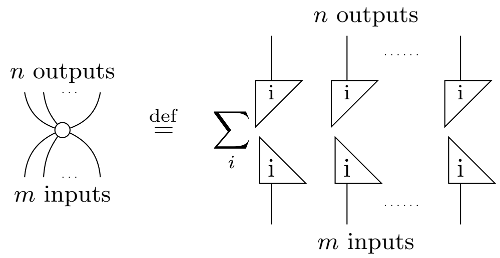
(12)

The diagrammatic proof is as follows,



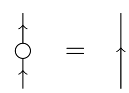
(13)

Spiders. A *spider* is a special linear operation from $\mathcal{H}^{\otimes m}$ to $\mathcal{H}^{\otimes n}$ that acts as a generalised Kronecker delta,



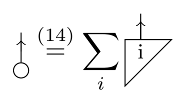
(14)

Any combination of incoming and outgoing arrows is possible. *The arrows on the wires are often omitted when there is no ambiguity.*
A special case of a spider is the spider with one input and one output, which equals the identity,



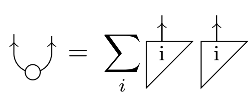
(15)

Another special case is the spider with zero inputs and one output. It is proportional to the equal superposition of all basis states.



(16)

A spider with two outgoing arrows corresponds to the maximally entangled state $\frac{1}{\sqrt{d}}\sum_i |ii\rangle$

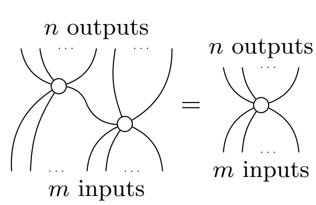


(17)

A spider that is not connected to any lines evaluates to a scalar, namely the dimension d of the Hilbert space,

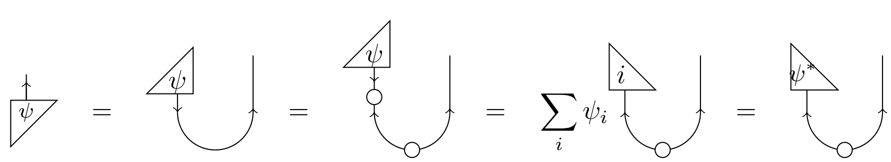
$$\bigcirc = \sum_i (\text{empty diagram}) = d. \tag{18}$$

An important property of spiders is that they fuse.



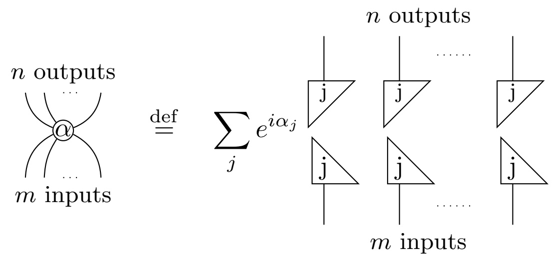
(19)

This follows directly from the definition (14). A spider is defined with respect to a certain basis. When that it not the standard basis, shading or colouring is applied, just as for basis states.
Equivalence between state preparation and EPR measurement.
There is a well known equivalence between on the one hand preparing a state $|\psi\rangle$ and on the other hand preparing a maximally entangled bipartite state followed by projecting one of the subsystems onto $|\psi^*\rangle$. In diagram notation this equivalence is visualised simply by bending a wire.



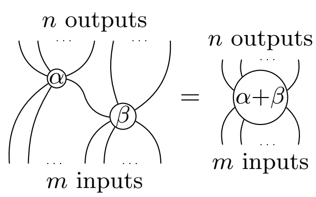
(20)

In the last diagram of (20) the spider creates the entangled state, and the complex conjugation $\psi \mapsto \psi^*$ is defined with respect to the spider's basis, i.e. $\psi_i \mapsto \psi_i^*$.
In case of a set of self-conjugate basis states the arrows on the wires do not have to be drawn, and the spider in the last diagram in (20) can be omitted, resulting in a simple picture consisting merely of the $\langle\psi^*|$ bra and a bent wire.
Phase spiders. Let $\alpha = (\alpha_i)_{i=0}^{d-1}$, with $\alpha_0 = 0$ by convention, be a vector containing angles. The α-phase spider is defined as



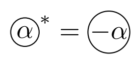
(21)

Phase spiders fuse like normal spiders, but their phases are added. This follows directly from definitions (14) and (21).



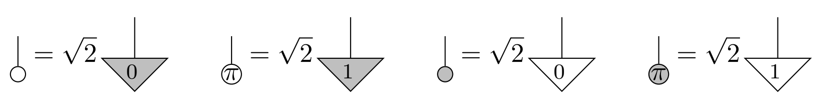
(22)

The complex conjugate of a phase spider has flipped phases.



(23)

Qubit states; Bloch sphere; switchable Pauli operations.
Qubit states ($d = 2$) correspond to spin states on the Bloch sphere. Typically the z-basis is chosen as the standard basis, with $|0\rangle = |+z\rangle$ and $|1\rangle = |-z\rangle$. The Pauli spin matrices are $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. A general spin state with spherical angles (θ, φ) is given by $\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$. The spin states along the x, y axes are given by $|\pm x\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$, $|\pm y\rangle = \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}}$. The '+' state in each case represents a logical 0.
In many qubit-based protocols it suffices to work with only the z-basis and the x-basis. The convention in [3, 5] is to use white colour for the z-basis and grey shading for the x-basis. The basis states are depicted as left-right symmetric, since they are real-valued when expressed in the standard basis. The following diagrammatic relations hold between the two bases,



(24)

Here a phase label π is shorthand for the two-dimensional phase vector $(0, \pi)$. Furthermore, a white π-spider with a single in- and output acts on a state like the Pauli operation σ_z, and a gray π-spider acts like σ_x.

(25)

Switchable σ_z and σ_x operations are built as follows.

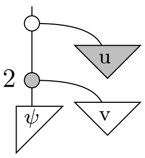
(26)

Here the $u \in \{0,1\}$ is a control bit that switches the Pauli operation.
Quantum One-Time Pad (QOTP) encryption [1, 4, 7] of a qubit state works with a two-bit key $(u,v) \in \{0,1\}^2$. The encryption operation E is

$$E_{uv}|\psi\rangle \stackrel{\text{def}}{=} \sigma_z^u \sigma_x^v |\psi\rangle \tag{27}$$

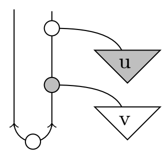
which can be depicted as

$$E_{uv}|\psi\rangle \quad \equiv \quad 2 \tag{28}$$



Bell states. The Bell states in two-qubit space are usually written as $|\Phi^\pm\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$, $|\Psi^\pm\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$. We write them in a slightly different way which displays the fact that the four Bell states are QOTP encryptions of each other, where the encryption acts on one of the two qubits,

$$|\Phi_{uv}\rangle = (\mathbf{1} \otimes \sigma_z^u \sigma_x^v)\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|0v\rangle + (-1)^u |1\bar{v}\rangle}{\sqrt{2}}. \tag{29}$$



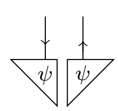
$$\equiv \quad \sqrt{2}|\Phi_{uv}\rangle. \tag{30}$$

2 Mixed states

Doubling. In the standard formalism, mixed states are described as positive semidefinite operators on the Hilbert space $\mathcal{H}$, with trace 1. The space of such *density matrices* is denoted as $\mathcal{D}(\mathcal{H})$. Because of the isomorphism

$$\mathcal{D}(\mathcal{H}) \cong \mathcal{H} \otimes \mathcal{H} \tag{31}$$

it is possible to express a mixed state, which is usually written in operator form [1] as $\tilde{\rho} = \sum_{ij} \rho_{ij} |i\rangle\langle j| \in \mathcal{D}(\mathcal{H})$, as an object in $\mathcal{H} \otimes \mathcal{H}$, namely $\rho = \sum_{ij} \rho_{ij} |i\rangle^* \otimes |j\rangle$. This has the advantage that it becomes possible to draw diagrams for mixed states in a way that is visually similar to pure states, i.e. creation of a mixed state has wires extending only upward, whereas an operator box has wires up and down. For a pure state $|\psi\rangle = \sum_i \psi_i |i\rangle$, whose density matrix is $|\psi\rangle\langle\psi| \in \mathcal{D}(\mathcal{H})$, this yields $\rho = \sum_{ij} \psi_i^* \psi_j |i\rangle^* \otimes |j\rangle = |\psi\rangle^* \otimes |\psi\rangle$, with diagram



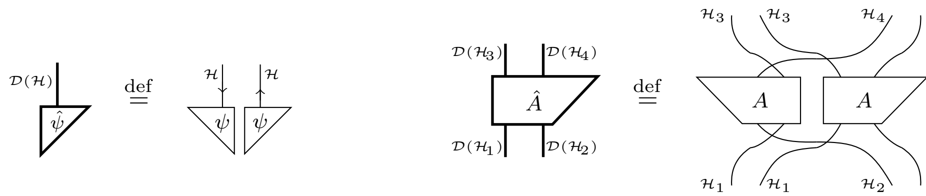
(32)

For brevity a special notation is introduced, in which a **thick-drawn** wire, spider, pure state or pure map[2] indicates **doubling** of the object as in (32), adding a complex conjugated copy to the left. Any thick-lined box/triangle means that it pertains to *mixed* states only. It is not possible to have

[1] We will use tilde notation for the operator form.

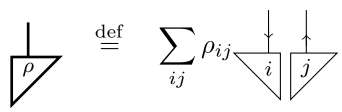
[2] A pure map is an operation on mixed states $\tilde{\rho} \in \mathcal{D}(\mathcal{H})$ that can be represented as $A\tilde{\rho}A^\dagger$, i.e. a linear operation on $\mathcal{H}$.

a thick box or spider connected to a thin wire. The special case of pure states and pure operations is indicated with a 'hat' notation,

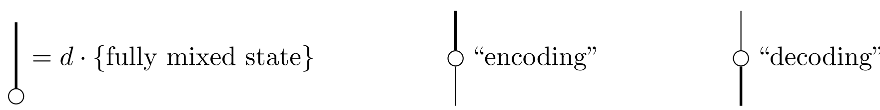


(33)

Thick spiders fuse just like thin spiders. Non-pure states ρ and non-pure operators A lack the left-right separated form, but can always be written in decomposed form, e.g.

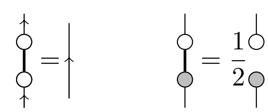

(34)

While it is not possible for a thick spider to connect to a thin wire, the reverse is possible (thin spider, thick wire) since two parallel identical thin wires may be interpreted as a thick one. The term 'bastard spider' is used for a thin spider connected to at least one thick wire. A number of important examples are shown below,

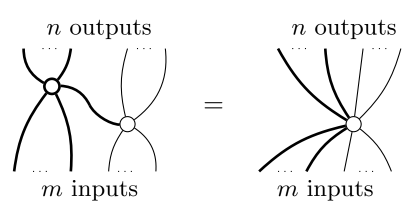


(35)

The 'encoding' operation creates the diagonal matrix element $|ii\rangle$ from the basis state $|i\rangle$; 'decoding' does the opposite. These operations allow for a description of quantum-classical systems such that thick wires represent quantum states and thin wires stand for classical states. (A classical value $i \in \{0, \ldots, d-1\}$ is transported as the basis state $|i\rangle$ on a thin wire). Encoding and decoding in the same basis acts as the identity. Decoding in a basis *complementary* to the encoding (orthogonal on the Bloch sphere) leads to a failure to convey data, which is diagrammatically visible as a **disconnect**,

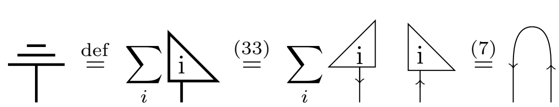

(36)

The fusion of a thin spider and a thick spider leads to a bastard spider.



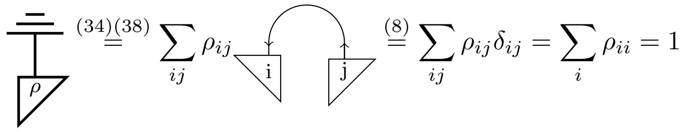
(37)

Taking the trace. The (partial) trace of a state is taken by connecting two whin wires that together make up a thick wire. This operation is depicted with the 'ground' symbol.



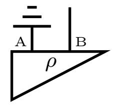
(38)

Another name for this operation is ‘discarding’, since the thick wire terminates. In the operator formulation of mixed states it holds that $\operatorname{tr}\tilde{\rho} = 1$. Diagrammatically this is expressed as



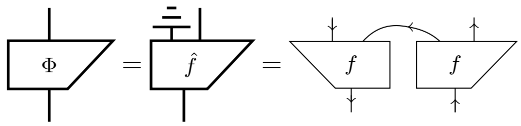
(39)

For a bipartite system, taking the partial trace $\operatorname{tr}_{\mathrm{A}}\tilde{\rho}^{\mathrm{AB}}$ to obtain the state of the ‘B’ subsystem is depicted as



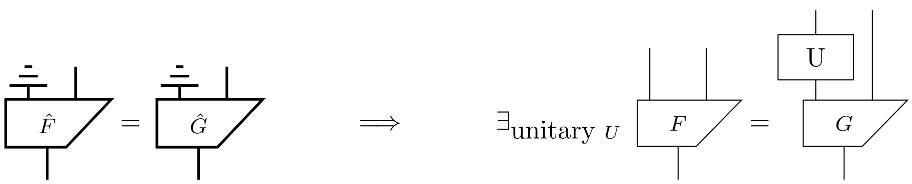
(40)

Similarly, a non-pure map Φ can be represented as a partially traced out pure map $\hat{f}$,



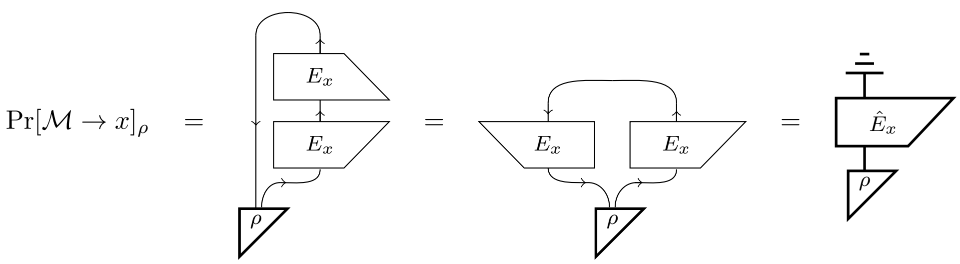
(41)

The purified f is unique up to a unitary operation applied to the traced-out wire. This leads to the following lemma,



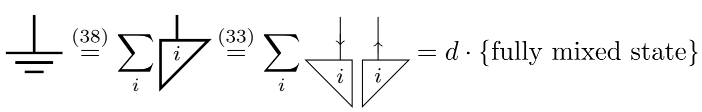
(42)

<u>Measurements</u>. In the **POVM** formalism (Positive Operator Valued Measure), a measurement $\mathcal{M}$ is described by a set of ‘elements’ $\{E_x\}_{x\in\mathcal{X}}$ acting on $\mathcal{H}$, with $\mathcal{X}$ the possible outcomes of the measurement. These elements satisfy $\sum_{x\in\mathcal{X}} E_x^\dagger E_x = \mathbf{1}$. Given a state $\tilde{\rho}$, the probability of outcome x is given by $\Pr[\mathcal{M} \to x]_{\tilde{\rho}} = \operatorname{tr} E_x^\dagger E_x \tilde{\rho}$; diagramatically this is depicted as



(43)

The Hermitian conjugate of *discarding* equals the preparation of the **fully mixed state**, up to a factor d.

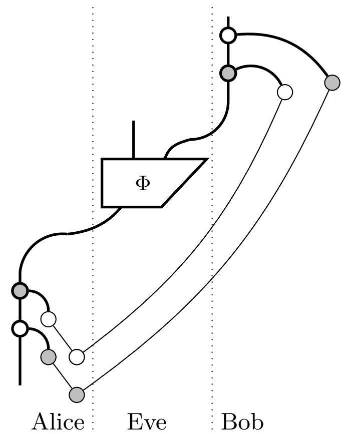


(44)

3 Protocols

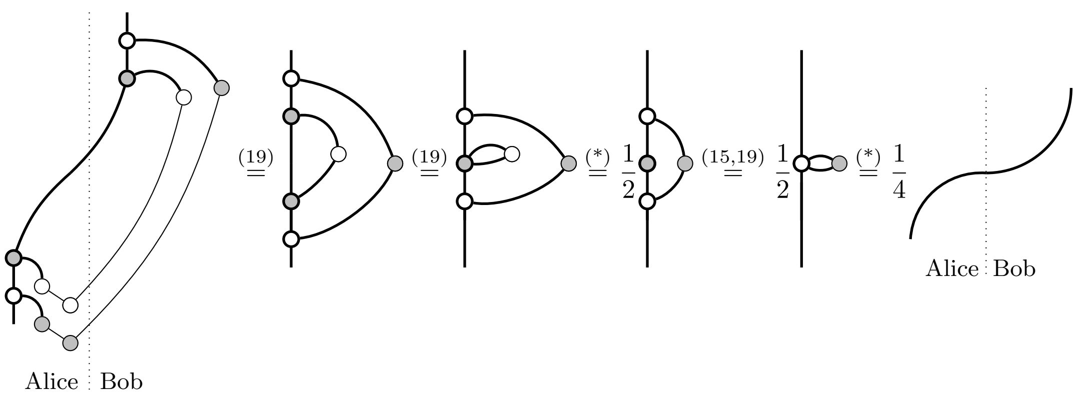
3.1 The Quantum One Time Pad

We showed the QOTP encryption step in (28). The full diagram for encryption and decryption of a qubit state (and including the most general attack that Eve could launch) is given below, up to a numerical factor 4.



(45)

The use of thick wires is necessary because (i) Eve's attack Φ is allowed to be very general; (ii) Alice may not know what state she is encrypting. The thin spiders connected to thin wires, at the bottom of the diagram, generate the two random key bits. One copy goes to Alice, one to Bob. Eve does not learn the key; this is visually clear, as the attack Φ does not have the key as input. The encryption by Alice is the doubled version of (28), with u and v replaced by the random bits from the thin spiders. Bob's decryption is the Hermitian conjugate of the encryption. **Correctness** of the scheme means that Bob correctly receives the state that Alice sent if Eve does not interfere. Diagramatically, correctness is proven by removing the Φ box and then using spider contraction rules to show that the protocol diagram reduces to a thick wire from Alice to Bob.



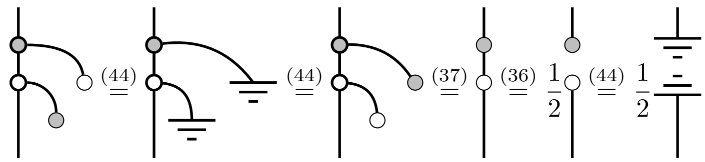
(46)

Step (*) consists of two parts: First, a double thin connection between complementary thin spiders yields a numerical factor 1/2 and a disconnect,[3] as we saw in (36); now we have a version of this situation where one of the spiders is doubled, yielding a factor 1/4 instead of 1/2. Second, the isolated thin spider yields a factor 2 due to the basis summation.

Security of the scheme means that Eve does not learn what Alice's state is. Diagrammatically, security is 'proven' by tracing out Bob and showing that the output of Eve's attack Φ is decoupled from Alice's input wire. Tracing out Bob removes the entire branch going from Alice to Bob. The

[3]We ignore a subtlety involving so-called 'antipodes' [3], which is allowed here because the antipode evaluates to the identity in the case of the combination of the x and z basis.

part of the diagram that serves as input to Φ reduces to

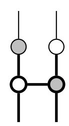


(47)

which indeed entirely disconnects Eve from Alice's state.

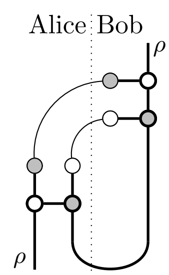
3.2 Teleportation

Alice holds a qubit state $|\psi\rangle$. Alice and Bob share an EPR qubit pair. Alice performs a measurement on her qubit $|\psi\rangle$ and her half of the EPR pair, in the Bell basis; this results in a two-bit measurement outcome (u, v). The two bits are communicated to Bob. Bob applies the Bell operation (u, v), which is essentially the decryption $\sigma_x^v \sigma_z^u$, to his half of the EPR pair. The end result is that Bob's qubit has state $|\psi\rangle$.
Measurement in the Bell basis is the Hermitian conjugate of the Bell state preparation (30) and can be depicted as



(48)

The thin wires carry the bits (u, v). The full diagram for teleportation of a state ρ is

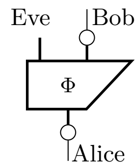


(49)

(Here the thick-wired 'cup' represents the creation of the EPR state $|\Phi_{00}\rangle$, i.e. we have omitted the spider that creates the EPR state.) By yanking the path of ρ (thick wire) to a straight line, the above diagram can be deformed such that it becomes precisely the leftmost picture in (46). Thus working with diagrams makes the equivalence between Quantum On-Time Padding and teleport particularly easy to visualise.

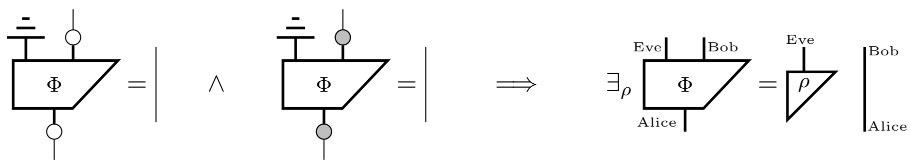
3.3 Quantum Key Distribution

We briefly discuss Kissinger, Tull and Westerbaan's diagrammatic treatment [5] of BB84 [2]. The main component of BB84 is the use of the quantum channel: Alice encodes a random bit x in a randomly chosen basis (standard basis or complementary) and sends it to Bob. Bob also selects one of these two bases at random and measures in that basis. Only the events where Bob's basis matches Alice's are relevant. Before reaching Bob, the qubit may be manipulated by Eve. Eve's attack is allowed to be anything at all, i.e. Eve may entangle her own quantum system with the qubit, and use quantum memory and quantum computation. The diagram for a single channel use (in the standard basis) is as follows.



(50)

Here Φ stands for the attack. The same diagram, but with grey spiders, applies to the other basis. *After* the attack Φ, Eve learns the basis choice and tries to exploit her quantum side information to guess the data bit sent by Alice. The statement that the protocol is secure[4] is formulated diagramatically as follows (Theorem 3.1 in [5]):

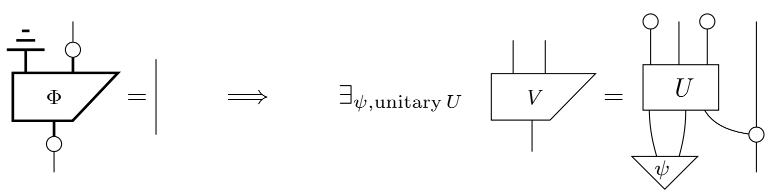


(51)

The two diagrams to the left of the implication arrow say that Alice and Bob see no disturbance in the two bases that they are using. The right hand side says that Eve is decoupled from the information that is going from Alice to Bob.

The proof of (51) consists of two parts. First, from the left hand side (non-disturbance) a rule is derived that allows one to pull spiders through the purification of Φ; here it is important that the rule applies only to those bases that are observed to have no disturbance, i.e. in BB84 the z-basis and x-basis. Second, an additional disconnected branch is pasted to Bob's wire and then all the spiders involved with Bob's wire are pulled through Φ. Here we will not write out the full proof from [5]; we highlight only one part of it that we will re-use in the diagrammatic reduction in Section 3.4.

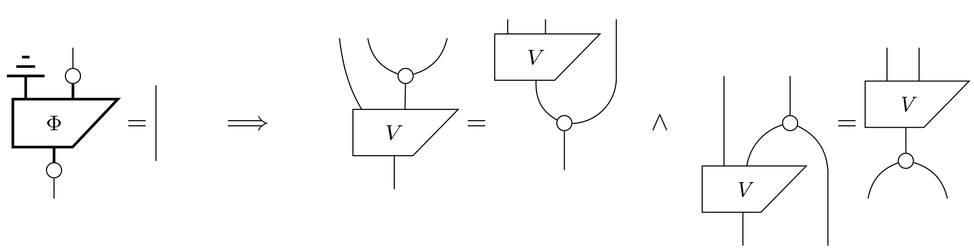
Lemma 1 *Let the white spider represent any orthonormal basis. Let V be a purification of* Φ*. It holds that*



(52)

<u>Proof</u>*: See the proof of Theorem 3.1 in [5].* □

Lemma 2 *Let the white spider represent any orthonormal basis. Let V be a purification of* Φ*. It holds that*



(53)

<u>*Proof*</u>: See the proof of Theorem 3.1 in [5]. □

(If Φ is not pure then the left output wire of V represents a space that is larger than Eve's Hilbert space; a part has to be traced out to obtain Eve's space.) Note that the third equation in (53) follows from the second equation by yanking down the rightmost wire.

[4]Here we show the noiseless case only. Noise is handled as in [5].

3.4 Eight-state encoding

Eight-state encoding was introduced in [8] as a technique for quantum-encrypting classical data, to be used in e.g. Quantum Key Recycling (QKR) protocols. The eight states are the QOTP encryptions of two specially chosen basis states:

$$|\psi_0\rangle \stackrel{\text{def}}{=} \cos\tfrac{\alpha}{2}|0\rangle + \sqrt{i}\sin\tfrac{\alpha}{2}|1\rangle \quad , \quad |\psi_1\rangle \stackrel{\text{def}}{=} \sin\tfrac{\alpha}{2}|0\rangle - \sqrt{i}\cos\tfrac{\alpha}{2}|1\rangle \tag{54}$$

where $\alpha \stackrel{\text{def}}{=} \arccos\frac{1}{\sqrt{3}}$ and $\langle\psi_a|\psi_b\rangle = \delta_{ab}$. On the Bloch sphere the $|\psi_0\rangle$ points in the direction $(1,1,1)$, and $|\psi_1\rangle$ in the direction $(-1,-1,-1)$. The QOTP-encrypted states are denoted as $|u,v,g\rangle$,

$$|u,v,g\rangle \stackrel{\text{def}}{=} E_{uv}|\psi_g\rangle = \sigma_z^u\sigma_x^v|\psi_g\rangle. \tag{55}$$

Their position on the Bloch sphere is depicted in Fig. 1.

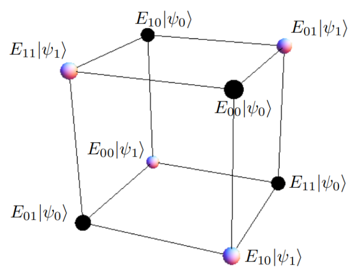
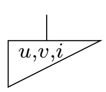
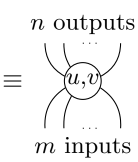


Figure 1: *The eight cipherstates $E_{uv}|\psi_g\rangle$ on the Bloch sphere, forming the corner points $(-1)^g\Big((-1)^u, (-1)^{u+v}, (-1)^v\Big)/\sqrt{3}$ of a cube.*

We label the four bases as (u,v). Instead of introducing four shadings or colors, we choose for a diagrammatic representation with labels,

$|u,v,i\rangle \equiv$ 

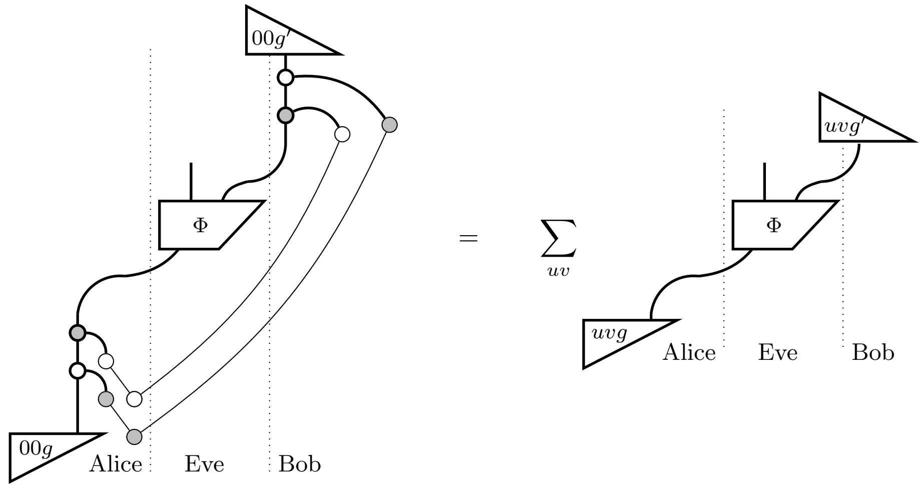
$\sum_i |u,v,i\rangle^{\otimes n}\langle u,v,i|^{\otimes m} \equiv$ 

(56)

The basis states are not depicted as left-right symmetric, since there is no basis in which all these eight states have a representation with real-valued vector components.

3.5 Security of eight-state encoding

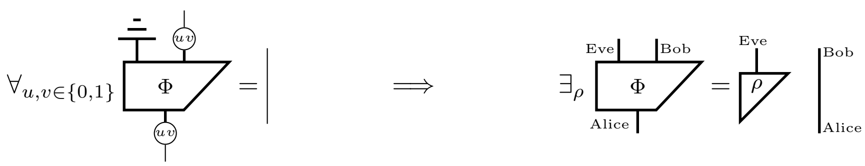
The diagram for encoding and decoding of a classical bit, plus Eve's attack, is essentially the diagram for QOTP of general states (45), but now the input is a classical bit encoded in the ψ_0, ψ_1 basis.



(57)

After the attack Φ, some information may leak about the basis (u, v) or the data bit g. Here too it is important that a security property like (51) holds [6]. The main result of this paper is that indeed this is the case.

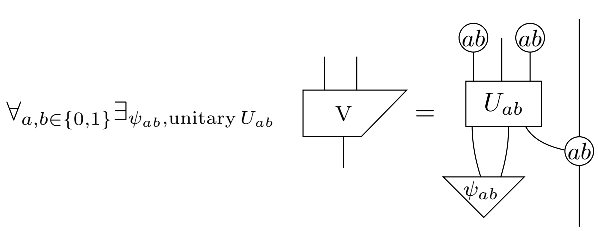
Theorem 1 (Main result) *Consider the encoding of classical data as in diagram (57). Let the label uv in a spider denote the (u, v)-basis in 8-state encoding. Non-disturbance in all four bases implies that Eve is decoupled from the Alice-to-Bob channel,*



(58)

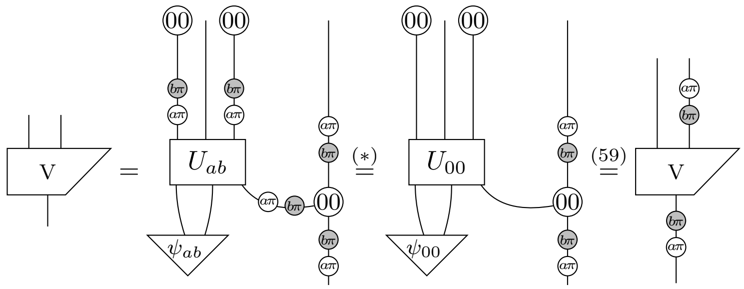
Proof: We follow an approach similar to the proof of Theorem 3.1 in [5]. The strategy is to make use of Lemma 2 by attaching a disconnect to the wire that goes from V to Bob, and then pull the disconnect through V. However, we cannot literally re-use the steps of [5] since our four bases are not mutually unbiased. Hence we cannot create a disconnect using (36); instead we will construct a disconnect using (47).

We start by first showing that a QOTP encryption can be 'pulled through" the purification of Φ. This is proven as follows. From Lemma 1 and the condition in the left-hand side of (58) we get



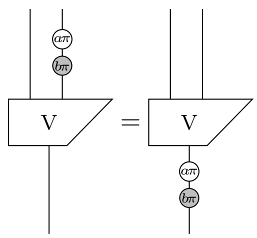
(59)

Writing the ab-spiders as encryptions of 00-spiders using phase spiders as in (26) yields



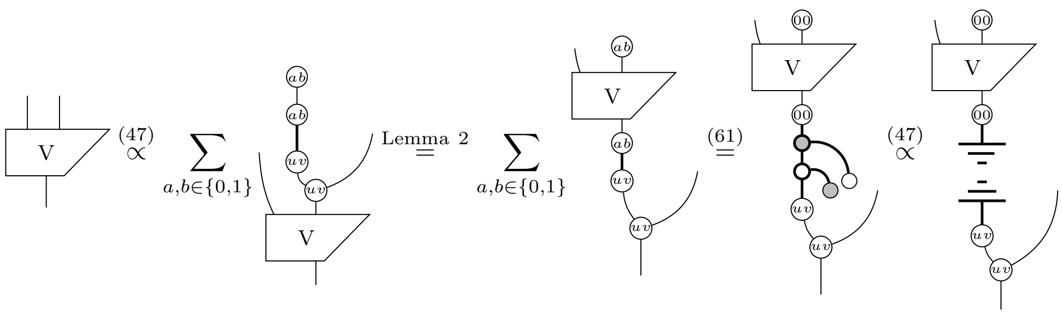
(60)

In the step (*) we used that pulling the ab-encryptions into the U_{ab} results in the U_{00}, ψ_{00} combination. From (60) it follows that



(61)

i.e. the encryption can be 'pulled through' V. Now we write, for any $u, v \in \{0, 1\}$



(62)

In the second diagram the two ab-spiders can be contracted; then the remaining ab-spider can be written as the ab-encryption of a 00-spider, which is turned into a disconnect by the $\sum_{ab}$. Then, the two uv-spiders fuse and form the identity operation. This explains why the second diagram is equivalent to the first. In the transition from the 3rd to the 4th diagram, both ab-spiders are rewritten as the ab-encryption of a 00-spider; then the topmost encryption operator is pulled through V and cancels the ab-encryption just below V.

Finally, in the last expression in (62) the trace on the uv-spider disappears and the two uv-spiders fuse to form the identity operator on the wire from Alice to Bob. Doubling the whole diagram yields the last expression in (58), with ρ being the doubling of V acting on a random input. □

The proof deviates from [5] in the way in which the disconnect is constructed in the second diagram of (62). Whereas the disconnect in [5] is based on complementary bases (36), we make use of QOTP encryption (47).

4 Discussion

Most of what is written in this document is extracted from [3] and [5], and rehashed into an introduction that we hope is appealing to physicists. Because of the peculiarities of 8-state encoding,

with basis states that do not allow for a simultaneous real-valued representation, we have chosen to explicitly show arrows on the wires in many of the diagrams.
The only really new content is Section 3.5, the diagrammatic proof that non-disturbance in 8-state encoding implies decoupling of Eve from Alice and Bob. The security of 8-state encoding is of course known, but the derivation with diagrams is novel.
Our diagrammatic treatment of 8-state encoding may be of interest for Symmetric Informationally Complete measurements ('SIC-POVM') for tomography.

We have covered only the noiseless case. The situation with channel noise can be dealt with in exactly the same way as BB84/6-state QKD [5]. Here it is important to note that the diagrammatic approach does not yield improved bounds (in fact they are worse than state-of-the-art). Instead of considering it as a numerical tool, we see diagrams as an intuitive visualisation aid that is simple to master yet powerful enough to derive security proofs.

Acknowledgements

We thank Aleks Kissinger and Daan Leermakers for useful discussions.

References

[1] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *41st Annual IEEE Symposium on Foundations of Computer Science*, pages 547—553, 2000.

[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*, volume 175, 1984.

[3] B. Coecke and A. Kissinger. *Picturing Quantum Processes.* Cambridge University Press, Cambridge, 2017.

[4] D.W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.

[5] A. Kissinger, S. Tull, and B. Westerbaan. Picture-perfect Quantum Key Distribution, 2017. `http://arxiv.org/abs/1704.08668`.

[6] D. Leermakers and B. Škorić. Optimal attacks on qubit-based Quantum Key Recycling. *Quantum Information Processing*, 17(3):57, 2018.

[7] P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.

[8] B. Škorić and M. de Vries. Quantum Key Recycling with 8-state encoding (The Quantum One-Time Pad is more interesting than we thought). *Int. J. of Quantum Information*, 15(3):1750016, 2017.

[9] Z. Wolffs. An introduction to a novel diagrammatic notation for quantum mechanics and its applications to some quantum cryptographic protocols, 2020. Bachelor thesis, Maastricht University, The Netherlands.