

An Interactive Learning Tutorial on Quantum Key Distribution

Seth DeVore and Chandralekha Singh

Department of Physics and Astronomy, University of Pittsburgh, Pittsburgh, PA 15260

Abstract: We describe the development and evaluation of a Quantum Interactive Learning Tutorial (QuILT) on quantum key distribution, a context which involves an exciting application of quantum mechanics. The protocol used in the QuILT described here uses single photons with non-orthogonal polarization states to generate a random shared key over a public channel for encrypting and decrypting information. The QuILT helps upper-level undergraduate students learn quantum mechanics using a simple two state system. It actively engages students in the learning process and helps them build links between the formalism and the conceptual aspects of quantum physics without compromising the technical content. The evaluations suggest that the QuILT is helpful in improving students' understanding of relevant concepts.

INTRODUCTION

Quantum mechanics is a particularly challenging subject for undergraduate students [1-10]. Based upon prior research studies that have identified difficulties [11-14], we have developed a set of Quantum Interactive Learning Tutorials (QuILTs) to help students develop a good grasp of quantum mechanics [15-19]. The QuILTs use an inquiry-based approach to learning in which students are asked a series of guiding questions and strive to bridge the gap between quantitative and qualitative aspects of learning quantum mechanics. They are developed based upon the findings of investigations of student difficulties in learning relevant concepts [20]. The instructors can use the QuILTs either as in-class tutorials on which students can work in small groups or as homework supplements. Here, we discuss the development and assessment of a research-based QuILT related to quantum cryptography on quantum key distribution (QKD) [21-30].

QKD is an interesting application of quantum mechanics useful for generating a shared secure random key for encrypting and decrypting information over a public channel [21-30]. QKD is already in use by the banking industry [29]. This real world application makes QKD a particularly useful vehicle for helping students learn about the fundamentals of quantum mechanics in an undergraduate course. A unique feature of secure QKD protocols is that two parties, e.g., a sender who is traditionally referred to as Alice and a receiver traditionally referred to as Bob, who generate a random shared key over a public channel, can detect the presence of an eavesdropper (traditionally referred to as Eve) who may be intercepting their communication during the shared key generation process to gain access to the key. Alice and Bob are connected via a quantum communication channel which allows quantum states to be transmitted during the random shared key generation process. When photon polarization states are used for shared key generation, the quantum communication channel used is generally an optical fiber or free space. In addition, during their shared key generation process, Alice and Bob also communicate certain information with each other via a classical channel such as the internet.

The ability to detect an eavesdropper in secure QKD protocols is due to the fact that physical observables are in general not well-defined in a given quantum state but measurement collapses the state and gives the observable a definite value. In particular, secure key generation exploits the fact that in general, measurement disturbs the state of a quantum mechanical system and that a random unknown quantum state cannot be cloned [31]. The indeterminacy is unique only to quantum mechanics and can be used to determine if someone eavesdropped during the QKD process and if so, how much information was gained by the eavesdropper, Eve. In particular, Eve must measure an observable in the state of the system sent by Alice to Bob during the shared key generation process over the public channel. But since quantum measurement in general disturbs the state of the system, she will not always know the state sent by Alice, and will be forced to guess the replacement quantum state to send to Bob at least some of the times she intercepts the communication between Alice and Bob by measuring Alice's transmitted state. Even if Eve intercepts what Alice transmitted and uses clever strategies for sending replacement quantum states, since she must guess the state to transmit to Bob at least in some cases, it will cause a discrepancy in the shared key that Alice and Bob generate in her presence. Also, if Bob is alerted by Alice that she has transmitted a state in the key generation process, and the

eavesdropper does not send a replacement state to Bob to replace what Alice had transmitted, the discrepancy present in the shared key will be such that Alice and Bob will detect the presence of an eavesdropper. After the entire shared key is generated over the public channel, Alice and Bob can compare certain bits, e.g., every p^{th} bit, to ensure that they agree on the shared key generated (they discard the bits they compare so that it is not part of the shared key). If they find discrepancy in the bits they compare (beyond a threshold discrepancy due to decoherence in actual situations), they will abort the shared key generated because someone may be eavesdropping.

The protocol discussed here that students learn via the QKD QuILT involves generating a shared key over a public channel using single photons with non-orthogonal polarization states (known as the B92 protocol [22]). The warm-up for the QuILT helps students learn background topics including the fact that in a two state system, a quantum state can be in a superposition of two linearly independent states but measurement of an observable will collapse the state and one obtains a definite value for the observable measured. In the first part of the QuILT after the warm-up, students learn about an insecure QKD protocol in which two orthogonal polarization states of single photons are used. Then they learn about the secure QKD protocol which uses two non-orthogonal polarization states of single photons via a guided inquiry-based approach to learning in which students are actively engaged in the learning process.

In the next section, we review the B92 [22] protocol (B92 is for the last name of the original inventor of the protocol, Bennett, and the year the protocol was published) students learn via the QKD QuILT. This is followed by an investigation of student difficulties with relevant topics and the development and evaluation of the QuILT. We then discuss the findings from the pretest, posttest, and a delayed posttest used to evaluate the effectiveness of learning relevant concepts via the QuILT in an upper-level quantum mechanics course. The pretest was administered after traditional instruction about the basic quantum mechanics required for QKD but before students worked on the QuILT. The posttest was administered after the QuILT and the delayed posttest was administered roughly two months after the QuILT [32].

THE QKD PROTOCOL STUDENTS LEARN

A classical key distribution protocol cannot guarantee that the key shared over a public channel is secure. Such a classical protocol depends on the computational difficulty of mathematical functions [30]. On the other hand, in order to securely generate a random shared key for encrypting and decrypting information over a public channel, QKD uses properties of quantum states and involves encoding information in quantum states. When measurement is performed in order to gain information, the state of the system collapses and one “bit” of information is obtained. In particular, the QKD protocols in general involve preparing and sending special quantum states and measuring an observable which yields one of two outcomes (either bit 0 or 1) in the prepared states with a certain probability. Though eavesdropping is possible for the secure quantum key generation protocol that students learn, comparing a small subset of the bits in the key at the end of the shared key generation process will reveal if an eavesdropper was present and if so, to what extent the key was compromised.

In the B92 protocol Alice randomly sends a series of single photons with either a $+45^\circ$ or 0° polarization. Bob examines each photon by passing it through a polarizer with a polarization axis of either -45° or 90° with a photodetector set up behind the polarizer which clicks if the photon passes through his polarizer. In the two possible cases in which the photon’s polarization is not orthogonal to the polarization axis of Bob’s polarizer, there is a 50% chance for the photon to pass through and a 50% chance for the photon to be absorbed. In the other two possible cases, in which the photon’s polarization is orthogonal to the polarization axis of Bob’s polarizer, there is a 100% chance for the photon to be absorbed. Therefore, on average, 25% of the time the photon will pass and be detected. Since the photon must not be polarized orthogonal to the polarization axis of Bob’s polarizer for it to pass through, Bob can determine the polarization of the photon when it passes through the polarizer and is detected by the photodetector behind the polarizer. If the photon is not detected by the photodetector, it could be polarized along either of the two possible directions (though it is more likely that it is polarized orthogonal to the polarization axis of Bob’s polarizer) and Bob cannot be certain of the polarization of the photon. Every time the photon is detected Bob contacts Alice over public channels and informs her that he detected that particular photon and both Alice and Bob record the polarization of that photon as the next bit in the key (e.g., they agree ahead of time that if Bob detects $+45^\circ$ polarized photon that Alice had sent, they will record +1 and if he detects 0° polarized photon she sent they will record a 0 for the shared key). If we introduce an eavesdropper (Eve) who is using the same protocol as Bob to intercept photons sent by Alice and replaces them to the best of her ability, she (like Bob) will not be certain of the polarization of photon that she intercepted 75% of the time (when her detector does not register the photon). Even if Eve makes the best guess for all cases in which she is not certain and assumes that the photon is polarized orthogonal to the polarization axis of her polarizer which will be correct in $2/3$ of these cases, she will send replacement photons with the incorrect polarization

of photon 25% of the time resulting in a discrepancy between Alice and Bob's key (which can be detected by Alice and Bob if they compare a subset of the total key over a public channel after the entire key is generated).

Before learning about the B92 protocol for secure key distribution involving two non-orthogonal polarization states of single photons, students learn about an *insecure* key distribution protocol using two orthogonal polarization states of single photons. In the insecure protocol, Eve can find out the polarization states of each photon that Alice sends to Bob while generating the shared key over a public channel with 100% certainty without her presence being detected by Alice and Bob. In particular, students learn that an eavesdropper in the insecure QKD protocol can generate a replacement photon with the same polarization as the one sent by Alice to Bob during the shared key generation process and transmit it to Bob without him realizing that the photon he intercepted did not come from Alice but came from Eve. The QuILT helps students learn that the ability for an eavesdropper to gain access to the key without her presence being detected makes this protocol insecure for generating a shared key over a public channel.

The QKD QuILT guides students through an ideal situation in the absence of decoherence. However, students learn that error can be introduced in the shared key generated by Alice and Bob due to decoherence as well (e.g., interaction of the photon with the surroundings which can change its polarization state or lead to scattering or absorption of the photon). They learn that the effect of decoherence can be neglected over small distances, e.g., QKD schemes, similar to the one they learn have been tested successfully and the highest bit rate system currently demonstrated exchanges secure keys at 1 Mbit/s (over 20 km of optical fiber) and 10 kbit/s (over 100 km of fiber) with applications in the banking industry [29].

STUDENT DIFFICULTIES

During the development of the QKD QuILT, we conducted 15 individual semi-structured think-aloud interviews [48] with physics undergraduate students enrolled in quantum mechanics and physics Ph.D. students to understand their difficulties with relevant concepts in order to effectively address them in the QuILT. During the semi-structured interviews, students were asked to verbalize their thought processes while they answered the questions about the QKD basics either as separate questions before the preliminary version of the QuILT was developed or as a part of the QuILT, which included various protocols for generating insecure or secure shared key over a public channel. Students were not interrupted during these think-aloud interviews unless they remained quiet for a while (if they became quiet they were asked to keep talking). After the students answered the questions to their satisfaction, we asked them for clarification of the issues they had not made clear earlier. In the interviews that were conducted before the development of the QuILT, students were asked general questions relevant for the QKD QuILT. In interviews conducted with different versions of the QuILT, students were asked to work on different parts of the QuILT including the basics while thinking aloud. In addition, students were also asked open-ended questions about issues relevant for QKD.

During the interviews throughout the development of the QuILT, some students claimed that the polarization states of a photon cannot be used as basis vectors for a two state system due to the fact that a photon can have infinitely many polarization state. They argued that since a polarizer can have any orientation and the orientation of the polarizer determines the polarization state of a photon incident on the polarizer, it did not make sense to think about polarization states of a photon as a two state system. These students were so fixated on their prior experiences with polarizers from introductory classes (which can be rotated to make its polarization axis whichever way one wants with respect to the polarization of incident light) that they had difficulty thinking of polarization states of a photon as vectors in a two-dimensional Hilbert space. It is interesting to note that most students who had difficulty accepting that two polarization states of a photon can be used as basis states for a two state system had no difficulty accepting that spin states of a spin- $\frac{1}{2}$ particle can be used as basis states for a two state system despite the fact that the two systems are analogous. Interviews suggest that this difference in their perception was often due to how a spin- $\frac{1}{2}$ system and polarization were first introduced to them and the kinds of mental models they had built about each of these systems. Generally, students are introduced to polarization in an introductory physics course in classical optics and they are introduced to spin- $\frac{1}{2}$ systems in a quantum mechanics course. Since students had learned about the spin- $\frac{1}{2}$ system only in quantum mechanics, thinking of spin states of a spin- $\frac{1}{2}$ particle as vectors in a two dimensional Hilbert space did not create a similar conflict. This difficulty in reconciling what students knew from classical optics about light passing through a polarizer and polarization states of a photon as vectors in a two dimensional Hilbert space is somewhat similar to the difficulty that introductory students have reconciling their everyday notions about force and motion with the established laws of physics learned in introductory physics courses.

As noted, some students who had difficulty connecting the measurement of polarization in a laboratory with polarization states of a photon were relatively comfortable with reasoning about measurement of a particular component of spin and thinking of spin states as vectors in a two-dimensional Hilbert space. During interviews, some

of them even mentioned that measurement of S_z will collapse a spin state which was initially in a superposition of eigenstates of \hat{S}_z to an eigenstate of \hat{S}_z . However, they had difficulty with similar reasoning about the measurement of polarization of a photon collapsing the polarization state which is initially in a superposition state (e.g., the simplest case, in a superposition of two orthogonal polarization states chosen to be parallel and perpendicular to the polarization axis of the polarizer) into an eigenstate of the polarization measured. Even after students were reminded that a spin state of a spin- $1/2$ particle can be in a superposition of eigenstates of \hat{S}_z and that eigenstates of \hat{S}_z can be used as basis states to write any state in this two dimensional Hilbert space, some interviewed students still had difficulty thinking of spin- $1/2$ and polarization states of photon as analogous and coming to terms with polarization states of a photon as vectors in a two dimensional Hilbert space. They had difficulty with the notion that we can associate a vector in the Hilbert space to correspond to any polarization state (which is an eigenstate of the corresponding polarization) and that any two orthogonal states in that space can be used as basis states to represent any polarization state. Interviews suggest that the difference in how students were first introduced to spin and polarization was at least partly responsible for why they often reasoned about these analogous two-state systems in very different ways.

Some written responses and interviews suggest that some students incorrectly thought that whenever single photons with a given polarization were sent through a polarizer, they would be completely blocked (absorbed) by the polarizer only when the photon polarization was orthogonal to the polarization axis. These students thought that a photon with any other polarization would make the photodetector behind the polarizer click. Individual discussions suggest that this difficulty was often related to the difficulty of applying the measurement postulate of quantum mechanics to the single photon incident on a polarizer situation. In particular, some of these students thought that a single photon incident on a polarizer can partly pass through the polarizer and partly get absorbed (e.g., for polarized photons, they thought that the cosine squared of the angle between the polarization axis of the polarizer and polarization of the photon yields the fraction of a photon that transmits as opposed to the probability of the photon being transmitted). They did not realize that a single photon will either get absorbed by the polarizer or it will pass through with a certain probability. Interviews suggest that this difficulty often had its origin in the fact that students were not considering single photons passing through a polarizer probabilistically and were interpreting the situation by mixing quantum mechanical and classical ideas. In particular, students often confused the situation of a single photon incident on a polarizer with that of a beam of light incident on a polarizer. They knew from classical optics that the intensity of light generally decreases after passing through a polarizer and is only completely absorbed if the polarization of incident light is orthogonal to the polarization axis of the polarizer and extrapolated this, incorrectly, to the single photon case.

Examining holistically, the written responses and interviews also suggest that some students felt that the polarizer will only block photons that are polarized perpendicular to the axis of the polarizer and will allow any other photons to pass through completely. On the other hand, other students thought that the polarizer will act in the opposite extreme, blocking all photons that are not polarized parallel to the axis of the polarizer. In the written responses, these two types of difficulties were less common but still serve to illustrate difficulties with the basics of how single photons interact with a polarizer, something that is important to help students understand the quantum mechanics principles at work in B92 QKD protocol.

A common difficulty before working on the B92 QKD protocol in the QuILT involves a lack of understanding of when both parties in the key generation process have successfully generated the next “bit” in the shared key in this protocol. Students with these difficulties did not realize that for each photon polarization that Alice sends, there is a non-zero probability of the photon being absorbed completely but only one of the two possible polarizations sent by Alice has a non-zero probability of being transmitted through each of Bob’s two polarizers that he randomly uses for his measurement. Often this difficulty resulted in students incorrectly assuming that it is possible for Bob to determine the polarization state of the photon Alice sent both if the photon is absorbed (not detected by the detector behind Bob’s polarizer) or transmitted (detected by the detector behind Bob’s polarizer). Students who had this difficulty often claimed that Bob will know the polarization of the photon if his detector does not click (as discussed earlier) due to their incorrect mental model that polarization of the photon must be perpendicular to the polarization axis of the polarizer for the photon to be completely absorbed. They also claimed that if the detector clicks they will know the polarization because a photon will be partly transmitted and partly absorbed (resulting in the detector clicking) in all situations in which the photon polarization is neither parallel nor orthogonal to the polarization axis of the polarizer. As a result of this difficulty, some students claimed that for all cases except when the photon polarization is perpendicular to Bob’s polarization axis in the given situation, Bob’s detector behind his polarizer would click. Due to these two difficulties, they incorrectly claimed that whether the detector clicks (signifying a photon passed through Bob’s polarizer) or not, the next “bit” of the key can be generated by the two parties.

Another relatively common way in which students misinterpreted when the next “bit” of the key is generated is that they thought that Bob is only certain about the polarization of the photon when the photon Alice sent is polarized

perpendicular to the polarization axis of his polarizer. These students incorrectly claimed that since photons with polarization perpendicular to the polarization axis of Bob's polarizer are always blocked, Bob must always know the polarization of the photon Alice sent when it is perpendicular to the polarization axis of the polarizer. In the case when photons are neither perpendicular nor parallel to the polarization axis of the polarizer, these students often claimed that since there is a non-zero chance for the photon to be either transmitted or absorbed, Bob cannot infer the polarization of the photon sent by Alice. Thus, these students incorrectly claimed that Bob can only generate the next bit of the key when there is only one possible outcome (when Bob's polarization axis is perpendicular to the polarization of the photon that Alice sends). These students did not realize that what is important is whether a given outcome (transmitted or absorbed) exists for both polarizations of photon that Alice could send or only for one of the polarizations. Bob knows about the photon polarization only when his photodetector clicks because his photodetector may not click when photons are absorbed which can occur for either of the two polarizations of the photons that Alice sends.

Students also had difficulty in distinguishing between a "qubit" and a "bit" and how a qubit can be in a superposition state but once a measurement of an observable is performed, we get one bit of information. Also, some students had difficulty in determining which angle was relevant for determining if the photon will pass through or get absorbed by a polarizer. In particular, these students were unsure whether the relevant angles were those between the polarization of the incident photon and the polarization axis of the polarizer. For example, some students always made use of the polarization of the photon with respect to the horizontal axis in order to determine the probability of transmission or absorption incorrectly.

THE DEVELOPMENT OF THE QUILT

The QKD QuILT began with an analysis of student difficulties with related concepts and how to help students develop a better understanding of these concepts. It builds on students' prior knowledge found via investigation of difficulties and uses a guided inquiry-based approach in which various concepts build on each other gradually. The development of the QuILT went through a cyclic interactive process which included the following stages [33]:

- (1) Development of the preliminary version based on a theoretical task analysis of the underlying knowledge and research on student difficulties with relevant concepts.
- (2) Implementation and evaluation of the QuILT by administering it individually to students and getting feedback from faculty members who are experts in these topics.
- (3) Determining its impact on student learning and assessing what difficulties were not adequately addressed by the QuILT.
- (4) Refinements and modifications based on the feedback from the implementation and evaluation.

As noted, in addition to written free-response questions administered to students in various classes, individual interviews with 15 students were carried out using a think-aloud protocol [34] to better understand the rationale for their responses throughout the development of various versions of the QuILT and the development of the corresponding pre-test and post-test, given to students before and after they engaged in learning via the QuILT. The QuILT asks students to predict what should happen in a particular situation and after their prediction phase is complete, they are provided a figure and table from which they can infer what they should have predicted. Then, they are asked to reconcile the differences between their prediction and what they infer from the information provided (in the latest version of the QuILT, students use a simulation [28] to check their prediction and then reconcile the differences between their prediction and what the simulation shows). After each individual interview with a particular version of the QuILT (along with the administration of the pre-test and post-test), modifications were made based upon the feedback obtained from students. For example, if students got stuck at a particular point and could not make progress from one question to the next with the hints already provided, suitable modifications were made to the QuILT. We also iterated all components of the QKD QuILT with three faculty members and made modifications based upon their feedback. The QuILT strives to provide enough scaffolding to allow students to build a good knowledge structure while remaining engaged in the learning process. The guided aspect of the QuILT is illustrated by one interviewed student noting that "[answers to] most of these [questions] I can figure out if I just think about it." When we found that the QuILT was working well in individual administration and the post-test performance was significantly improved compared to the pre-test performance, the QuILT was administered in class. On average, students spent around 1.5 hours on the entire QuILT. It appeared that by working through the QuILT, most students had developed a good grasp of the concepts involved in the quantum key distribution protocol.

QKD QuILT (Based on B92 Protocol)

The QuILT warm up first helps students learn the basics related to bits, qubits, polarization states of a photon, and effect of measurement on a two state system. Many of these basics are asked in a series of multiple choice questions in a guided approach to learning. The need for reinforcing these basics in a guided approach was evident from answers to written free-response questions and during individual interviews with students. For example, after going over the basics, one interviewed student noted “If I hadn’t known the stuff in the basics I would be really confused with the QKD part”. The following questions (not necessarily consecutive) in the basics section help students learn about a qubit:

Q: The quantum-mechanical analogue of a classical bit is called a “qubit”. A qubit can be described as $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ where $|0\rangle$ and $|1\rangle$ are two orthonormal states of a quantum system and α and β are two complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Let \hat{Q} be an operator corresponding to a physical observable such that $\hat{Q}|0\rangle = 0|0\rangle$ and $\hat{Q}|1\rangle = 1|1\rangle$. Choose all of the following statements that are correct:

- (I) A bit cannot be in both $|0\rangle$ and $|1\rangle$ states. However, a qubit can be in a superposition of $|0\rangle$ and $|1\rangle$ states.
- (II) A measurement of observable Q in a state $|q\rangle$ can only produce one of two possible values.
- (III) When you perform a measurement of Q in a qubit, you obtain one bit of information.

Q: Choose all of the following that can form a qubit (i.e., that can be used as basis states for a qubit):

- (I) the eigenstates of \hat{S}_z for a spin one-half particle
- (II) the two orthogonal polarization states of a photon
- (III) the ground state and the first excited state of a one dimensional infinite square well.

We find that discussing these kinds of questions with other students while working on the QuILT in small groups helps students grasp the basic concepts that are necessary to understand how quantum key distribution works and why a particular protocol is secure or insecure. The following question is also asked in the warm up (basics section) after a series of questions about specific polarization states of a photon:

Q: If a single photon with a normalized polarization state $|S\rangle = \alpha|H\rangle + \beta|V\rangle$ is incident on a horizontal polarizer, which one of the following is true?

- (a) The photon passes through the polarizer with a probability $|\alpha|$.
- (b) The photon passes through the polarizer with a probability $|\beta|$.
- (c) The photon passes through the polarizer with a probability $|\alpha|^2$.
- (d) The photon passes through the polarizer with a probability $|\beta|^2$.

Once students work through the basics, they are first led through the *insecure* protocol using orthogonal polarization states of photons. They learn that the protocol is not secure due to the use of orthogonal polarization states and eavesdropping will go undetected. In this protocol, students are led through a series of questions without the eavesdropper. Then, they are asked about Eve’s interference. Students are guided to realize that Eve is capable of intercepting and replacing photons without being detected. This insecure protocol gets students used to the process by which a shared key can be generated but illustrates a flawed method that is prone to eavesdropping going undetected.

Next, students are guided through the B92 protocol which generates a secure key in which Alice, Bob and Eve each use two non-orthogonal polarization states of a photon. Following the basics, students are guided through a series of questions in which there is no eavesdropper. These questions culminate in Table 1 that students complete which spans all possible combinations of Alice’s polarization, Bob’s polarization and whether or not Bob’s detector clicks. In each situation, students are asked if a bit is recorded by Alice and Bob and if so which bit is generated (0 or 1). After completing this table in which students predict what should happen in each situation, they were provided with a figure that illustrates what should happen in a given situation (Figure 1). Figure 1 displays the probabilities that a bit is recorded in each case. Students are then guided to address cases in which Eve has eavesdropped on the key generation process. The questions culminate with students calculating that Eve will introduce an error in 25% of the bits that Bob records (in the ideal case with no decoherence, eavesdropping is the only source of error). They learn that if Alice and Bob compare a small subset of the shared key after the entire key is generated,

Table 1. In the B92 protocol in the QuILT, students are asked to complete the empty boxes in the table below predicting what should happen in a given situation based upon their understanding of the QKD protocol involving non-orthogonal polarization states of a photon.

Alice's polarization:						
Bob's polarization:						
Bob's detector clicks:	N	N	Y	N	N	Y
Bit is recorded: (Y or N)						
Which bit they record: (0 or 1 or -)						

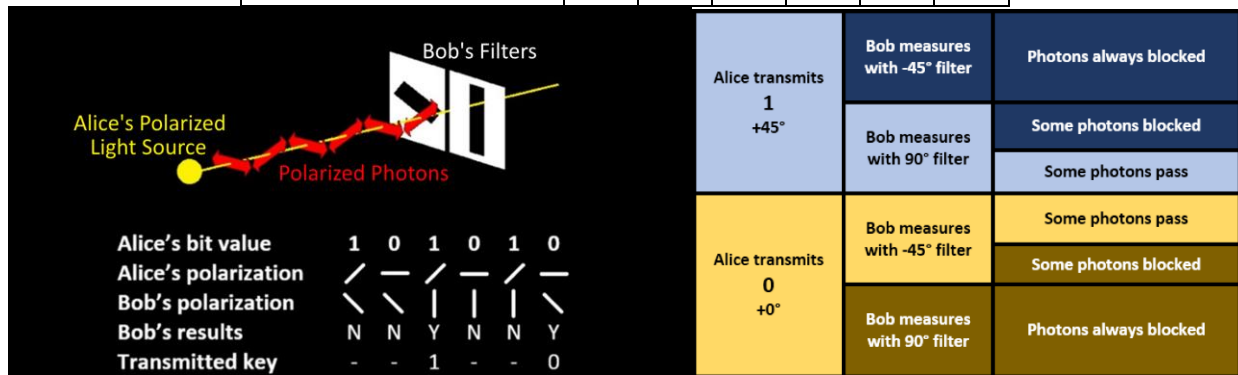


Figure 1. In the QuILT, students are first asked to make predictions about what should happen in a given situation and later asked to check whether their predictions are consistent with the information in this figure about the B92 QKD protocol involving non-orthogonal polarization states of single photons. Students are then asked to reconcile differences between their predictions and what happens in a given situation if their predictions are not consistent with this figure before they proceed.

they will know that this error is due to eavesdropping and they will discard the key and attempt the key generation process at another time, preferably through other channels. The following is an example of a question students answer as the culmination of a series of questions regarding Eve's interference in the key generation process:

Q: When Eve's detector does not click after she intercepts Alice's photon, she is not sure about the polarization of the photon sent by Alice. Eve will have to guess the polarization of the replacement photon she will send to Bob (in place of the one she intercepted). Suppose Eve is intercepting every photon sent by Alice and sending a replacement photon to Bob. Choose all of the following statements that are correct about the strategy for sending replacement photons to Bob when Eve is not sure what she intercepted from Alice:

- (I) If Eve's polarizer is at 90° when she intercepted the photon sent by Alice and the detector does not click, she has less chance of making an error if she sends a replacement photon with 0° polarization to Bob.
- (II) If Eve's polarizer is at -45° when she intercepted the photon sent by Alice and the detector does not click, she has less chance of making an error if she sends a replacement photon with 45° polarization to Bob.
- (III) If Eve's polarizer is at 90° and the detector does not click, she has the same chance of making an error regardless of whether she sends 0° or 45° polarization photon to Bob to replace it.

RESULTS FROM THE PRETEST, POSTTEST, AND DELAYED POSTTEST

Students worked on the QKD QuILT in class in small groups in an upper-level undergraduate quantum mechanics course intended for physics majors. Before the QuILT, students learned about polarization states of photons and a basic outline of quantum key distribution. Students were administered the pretest before working on

Table 2. Pretest, posttest, and delayed posttest results for the QKD QuILT broken down by question. The pretest (posttest) results are based on answers of 74 (76) students with an average score of 52.7% (90.9%). The delayed posttest results are based on answers from 24 students.

Question #	% Correct on Pretest	% Correct on Posttest	% Correct on Delayed Posttest
1	51.4	93.4	-
2	63.5	92.1	79.2
3	41.9	90.8	-
4	63.5	98.7	-
5	52.7	98.7	83.3
6	48.6	78.9	-
7 Box 1	71.6	97.4	-
7 Box 2	45.9	96.1	-
7 Box 3	47.3	93.4	-
7 Box 4	79.7	98.7	-
8	13.5	61.8	-
Average	52.7	90.9	-

the QuILT and they were given the full quiz score for trying their best on the pretest. The posttest was administered in the next class after all students had the opportunity to complete the QuILT at home if they did not finish it in class and it was counted as a quiz. The delayed posttest was given to students roughly two months after the QuILT. The pretest and posttest are identical in structure with only the polarization angles changed between the pretest and posttest. The pretest and posttest each begin by briefly outlining a situation similar to the B92 protocol to ensure that the students are familiar with it. The pretest (and posttest) then asks a series of questions regarding a B92 protocol setup with Alice's polarization axes randomly switched between 70° or 0° (60° or 0° for the posttest) and the polarizer axes for Bob randomly switched between -20° or 90° (-30° or 90° for posttest). The delayed posttest was comprised of two questions that were similar in structure to two questions present on the pretest and posttest with the only difference being the angles used. For the delayed posttest Alice's polarization axes randomly switched between 50° or 0° and the polarizer axes for Bob randomly switched between -40° or 90° . Table 2 shows that student performance increases from roughly 53% on the pretest to roughly 91% on the posttest. Below, we discuss student performance on each question separately (see Table 2).

Q1: Bob uses the polarizer with a -20° polarization angle and his photodetector does not click. Choose all of the following statements that can be inferred based upon the above protocol used by them:

- (I) Bob is 100% sure about the polarization of the photon sent by Alice.
- (II) Alice must have sent a photon with a 70° polarization.
- (III) Alice must have sent a photon with a 0° polarization.
- (IV) None of the above.

This question evaluates students' understanding of when a bit of the key cannot be generated. Since the detector does not click, Bob cannot infer anything about the polarization of the photon Alice sent and thus cannot use this photon to record the next bit making the correct answer "None of the above". Examining the pretest data, we note that roughly 50% of students incorrectly claimed that a "bit" of the key can be generated even when no photon is detected. After working on the QuILT, practically no students had this difficulty. The major difficulty that was common in this question was discussed in the student difficulties section earlier. In particular, some students incorrectly claimed that the photon that Alice sent is polarized perpendicular to Bob's polarizer and Bob is 100% sure about the polarization of the photon sent by Alice.

Q2: Bob uses the polarizer with a -20° polarization angle and his photodetector clicks. Choose all of the following statements that can be inferred based upon the above protocol used by Alice and Bob:

- (I) Bob is 100% sure about the polarization of the photon sent by Alice.
- (II) Alice must have sent photon with a 70° polarization.
- (III) Alice must have sent photon with a 0° polarization.

This question supplements the first question. It evaluates student understanding of when a “bit” of the key can be generated. When the photodetector clicks, Bob knows that the photon that Alice sent cannot be polarized perpendicular to Bob’s polarizer and therefore he can determine the polarization of the photon he detected, so that the correct answer is “(I) and (III) only”. The number of students who answered this question correctly on the pretest is likely to be somewhat inflated due to one of the common incorrect models that students used to describe QKD that leads students to select the correct answer due to incorrect reasoning. These students thought that the polarizer only blocked photons that were polarized perpendicular to its axis and that all photons that were not perpendicular to its axis were allowed to pass through (either fully or partially) causing the detector to click. Thus, they would answer that Bob knows the polarization of the photon that Alice sent and that the photon has the polarization which is not perpendicular to the axis of the polarizer that Bob used. Though these students made the correct selection from the options given, they incorrectly thought that this setup will always result in Bob’s detector clicking. Table 2 shows that about 40% of students failed to answer this question correctly on the pretest but very few student had this difficulty after working on the QuILT. Even in the delayed posttest after two months, student performance is significantly better than the pretest.

Q3: Suppose Alice transmits a photon with 70° polarization. Bob uses a polarizer with 90° polarization angle to intercept it. Write down the probability that the photon will pass through Bob’s polarizer.

This question evaluates student understanding of how a polarizer interacts with single polarized photons. Students must know that the probability of a photon passing through a polarizer is $\cos^2 \theta$ where θ is the difference between the polarization of the photon and the polarization axis of the polarizer ($\cos^2 20^\circ$). Two common student difficulties became apparent on the pretest. The first involved students using $\sin^2 \theta$ rather than $\cos^2 \theta$ which suggests a lack of understanding of the transmission probability through a polarizer for a polarized photon. The second difficulty was identifying the angle in the equation for transmission probability incorrectly. Many students selected one of the angles provided in the problem statement rather than taking the difference between photon polarization and the polarization axis of Bob’s polarizer. These two difficulties and other less common mistakes resulted in more than half of the students failing to correctly answer this question on the pretest. After the QuILT, very few students made a mistake on this question.

Q4: Alice transmits a photon with 0° polarization and Bob uses a polarizer with -20° polarization angle. Which one of the following statements is true?

- (a) The photon is blocked by Bob’s polarizer with a 100% certainty.
- (b) The photon will pass through Bob’s polarizer with approximately 88.3% likelihood.
- (c) The photon will pass through Bob’s polarizer with approximately 11.7% likelihood.
- (d) The photon will pass through Bob’s polarizer with a 100% certainty.

Question 4 investigates student understanding of the likelihood that Bob’s polarizer would block the photon with a given polarization. Question 4 closely parallels question 3 and requires that students calculate the probability of a photon passing through the polarizer to be roughly 88.3%. Similarly to question 3, there are two major difficulties that students have with this question. One difficulty which was discussed earlier stems from using $\sin^2 \theta$ rather than $\cos^2 \theta$ to predict the probability of transmission. The second difficulty involves assuming that the photon is either always transmitted or always absorbed despite the fact that photon polarization and the polarization axis of Bob’s polarizer are neither orthogonal nor parallel. These difficulties resulted in roughly 40% of students answering this question incorrectly in pretest. Table 2 shows that after working on the QuILT, practically none of the students answered this question incorrectly.

Q5: Bob uses a polarizer with 90° polarization angle and the detector does not click. Can he infer the polarization state of the photon that Alice sent? If so, what is it?

- (a) Yes. Alice must have sent a photon with 0° polarization.

- (b) Yes. Alice must have sent a photon with 70° polarization.
- (c) No. Alice could have sent a photon with either polarization (0° or 70°).
- (d) None of the above.

Question 5 examines concepts similar to those examined in Question 1. The primary concept emphasized in this question involves understanding that the photon’s polarization state, and thus the next “bit” of information, can be determined only when the detector clicks, so that the correct answer is option c. Two of the available options assert that the polarization of the photon that Alice sent can be determined and is one of the two possible polarization angles. A third option, “none of the above”, is logically unsound because the question statement gives every piece of information that Bob has in this situation meaning that he must be able to make some sort of determination, as he would during key generation. These three distracting options lead to roughly half of students selecting the incorrect answers in the pretest. The most common choice is based on the same common difficulty that students had with question 1. These students claimed that the photon is only blocked when the polarization of the photon is perpendicular to the axis of the polarizer and therefore they select the option that states that Bob can identify the polarization of the photon and that it is polarized perpendicular to the axis of his polarizer. After working on the QuILT, almost all students answer this question correctly. Table 2 shows that after two months slightly over 15% of students answered this question incorrectly.

Q6: Choose all of the following statements that are correct based upon the protocol described:

- (I) Whenever Bob’s detector clicks, he can infer the polarization of the photon that Alice sent.
- (II) Whenever Bob’s detector does not click, he cannot infer the polarization of the photon that Alice sent.
- (III) If Alice sends a photon with 0° polarization and Bob uses a polarizer with -20° polarization angle, that photon will be partly absorbed and partly transmitted.

This question evaluates student understanding of several important concepts relevant for the B92 protocol. It simultaneously tests whether students understand that if Bob’s detector clicks, the polarization state of Alice’s photon can be determined and thus the next bit of the key can be generated and if the detector does not click, the polarization state of the photon Alice sent cannot be inferred. Thus, the correct answer is “(I) and (II) only”. This question also includes a good distractor related to a common difficulty students have before the QuILT, namely, that a single photon can be partly absorbed and partly transmitted (as discussed in the difficulty section earlier, this difficulty was often a result of over generalization of the fact that when a beam of light passes through a polarizer, the intensity of light generally decreases due to some light getting absorbed and some passing through). About half of the students selected the correct answer in the pretest. The two most common incorrect answers are based on two similar difficulties discussed earlier. Both difficulties involve Bob being able to determine the polarization of the photon that Alice sent regardless of whether the detector clicks or not. Students were often confused about what happens to photons that are polarized neither perpendicular nor parallel to the axis of the polarizer. They incorrectly thought that the photon is either partially transmitted and partially absorbed resulting in the transmitted portion of the photon making the detector click or that they are completely transmitted allowing the detector to click. Table 2 shows that after the QuILT, roughly 80% of students correctly answered this question.

Q7: Complete the third column of the following table by recording “the probability that a photon will pass through and hence Bob’s detector clicks”:

		Probability of detector clicking
Alice transmits 70°	Bob uses -20° polarizer	
	Bob uses 90° polarizer	
Alice transmits 0°	Bob uses -20° polarizer	
	Bob uses 90° polarizer	

Since this exercise only requires students to take the difference between the two angles and use it with the equation for the probability that the photon will be transmitted ($\cos^2 \theta$, which is 0%, approximately 88.3%, 88.3% and 0%, respectively) it is reasonable to expect some uniformity across these four questions. Upon examining the pretest data in Table 2, we observe that the percentage of students who correctly answered each sub-question ranges from roughly 50% to 80%. One reason for the range of correct answers is that many students did not know the

expression for the probability that the photon will be transmitted, but they knew that a photon will not pass through an orthogonal polarizer. After working on the QuILT, nearly all of the students answered these four questions correctly.

Q8: Using the table above for the case described in the preceding question, calculate the percentage of measurements in which Bob is 100% sure about the polarization of the photon that Alice sent out of all of the experiments that Alice and Bob conduct.

The primary difficulty on this question was to properly account for each of the four probabilities in the table to determine the overall probability of roughly 44.2%. In particular, several students ignored any probabilities from the table that were equal to zero and proceeded to average the remaining probabilities. Other students simply wrote down 50% due to there being a nonzero probability of generating a bit of the key 50% of the time. A slightly less common error that several students made involved multiplying the nonzero probabilities together to determine the average probability of generating a shared bit of the key. Table 2 shows that slightly over 10% of students answered this question correctly on the pretest while roughly 60% of students determined this probability correctly on the posttest.

Overall Results for the Pretest, Posttest, and Delayed Posttest

The pretest and posttest responses suggest that many students have several alternative models of concepts relevant for QKD and they have difficulty with various concepts including the polarization states of a single photon and the single photon state upon measurement. These alternative models are predominantly observed in student responses on the pretest. For example, one of these alternative models is suggested by students claiming that a photon will only be blocked by a polarizer if its polarization angle is perpendicular to that of the photon polarization. This model results in students claiming that if the detector does not click, the polarization of the photon must be perpendicular to that of the polarization angle of the polarizer. Therefore, these students incorrectly claimed that a bit of the key can be generated every time a photon is sent to Bob. Additionally, use of this incorrect model will result in students answering questions about when Bob's detector will click correctly without correct reasoning.

A second model that is less commonly used by students includes the notion that only photons that are polarized parallel to the polarization axis of the polarizer are able to pass through and make the detector click. This model results in neither of the two possible polarizations of photon that Alice sends to Bob making Bob's detector click. We find that the students using this model generally had additional difficulties regarding when a bit of the shared key can be generated.

In addition, examination of students' responses (especially across the pretest questions) reveals inconsistencies in student reasoning. One set of inconsistencies is displayed by student responses to Questions 3, 4 and 7. Despite the fact that Questions 3 and 4 are nearly identical questions and are both contained within the answers to Question 7, it was common on the pretest to find an answer for one of these three questions that did not match the pattern being followed in the other two questions and in some cases the boxes for Questions 7 that were supposed to be similar to responses to Questions 3 and 4 had different student responses. Another common inconsistency is found when examining the responses to Questions 1 and 5 on the pretest. Despite these two questions being nearly identical to each other in subject matter, students often selected inconsistent responses to these questions. On the pretest, even on other questions student reasoning was often inconsistent.

Interviews suggest that one cause of inconsistency across answers is the context of the questions. For example, when students are asked questions that require conceptual answers and require no equations or mathematical manipulations (e.g., Questions 1, 2, 5 etc.), they are more likely to answer them based upon their alternative model. If instead they are asked a question that requires a mathematical answer, e.g., the probability of a photon passing through a polarizer (e.g., Questions 3, 4, 7 etc.), students are likely to rely on equations even if the results disagree with their model (students may not even compare these answers with their model to check for consistency). Other subtle changes in the context also affect student responses to similar questions. When comparing Questions 1 and 5, the major difference is the change in the layout of the available answers but it was enough to cause students to answer these two questions inconsistently, especially on the pretest. Interviews suggest that some students on the pretest became overly focused on the details of each individual question. In the more extreme cases, this was taken to the point where students answered each question without thinking about its interrelation with other questions. This type of treatment was at least partly responsible for students answering Questions 3 and 4 differently than Question 7 (which requires the answers to Questions 3 and 4). Students became too focused on each individual question and did not check for consistency across questions.

Students' posttest responses are significantly more consistent across questions. Interviews and written responses suggest that the QuILT also improves student understanding of polarization states of a photon and how to make connection between a polarizer in a physical space and polarization states of a photon in a Hilbert space. It also helps students think about single photons as having a probability of transmission or absorption rather than being partially transmitted and partially absorbed. The QuILT helps students understand that quantum measurement collapses the polarization state of a photon depending upon the polarizer used. As noted, before the QuILT, many students claimed that only a photon with a polarization orthogonal to the polarization axis of the polarizer will get completely absorbed and the photodetector does not click only for the case in which the photon polarization is orthogonal to the polarization axis because in all other cases the photon will partly get transmitted and partly get absorbed. Moreover, they incorrectly inferred that since the photodetector will not click only for the case in which the polarization axis of the polarizer and the polarization of the photon are orthogonal, Bob will know the polarization of the photon Alice sent only for the case in which the photodetector does not click. Overall, the QuILT was helpful in improving student understanding of topics emphasized.

The delayed posttest results show that despite the scores not remaining as high as they are for the posttest given immediately after the QuILT they are markedly higher than student scores on the pretest for both of the questions examined. The two questions that make up the delayed posttest were selected as particularly good examples of questions that require an understanding of QKD and quantum mechanics principles related to the B92 protocol to answer. Thus, the QuILT is effective at improving student understanding of QKD and the associated quantum mechanics principles over an extended period of two months.

SUMMARY

We developed and evaluated a QuILT to help upper-level undergraduate students learn quantum cryptography in the context of quantum key distribution using B92 protocol [22]. The B92 secure QKD protocol that students learn in the QuILT uses generation of a shared key securely over a public channel using two non-orthogonal polarization states of single photons. Alice randomly sends single photons with one of the two non-orthogonal polarization states (e.g., with 0° and 45° polarization states) and Bob randomly intercepts the single photons with one of two non-orthogonal polarization states (e.g., randomly with 90° and -45° polarization states if Alice randomly transmits 0° and 45° polarized photons) together with a 100% efficient photo-detector behind his polarizers to detect the photons transmitted by Alice. After the measurement of polarization, the photon is polarized in the state it was measured, with all information about its initial polarization lost. A systematic comparison, e.g., of every p^{th} bit in the shared key, after a sufficiently long key is generated by each person will display at least a minimum threshold error if Eve was eavesdropping no matter how innovative her protocol for replacement of photon is.

The QKD QuILT provides a guided approach to bridge the gap between the quantitative and conceptual aspects of quantum mechanics. It keeps students actively engaged in the learning process and evaluation shows that the QuILT improves students' understanding of concepts related to the QKD. Performance on the QuILT pretest showed that students were able to answer only slightly over half of the questions about the B92 protocol after a typical classroom treatment of the quantum mechanics principles related to this protocol. After working through the QuILT, student understanding of the B92 protocol and the associated physics principles were improved such that the average score was roughly 90% on the posttest. Finally, a survey given at the end of the semester shows that students found the QKD QuILT to be exciting and rated it highly.

ACKNOWLEDGEMENTS

We thank the US National Science Foundation for award PHY-1202909.

REFERENCES

1. P. Jolly, D. Zollman, S. Rebello, and A. Dimitrova (1998). Visualizing potential energy diagrams, *Am. J. Phys.* **66**(1), 57-63.
2. Muller, R and Wiesner, H 2002 Teaching quantum mechanics on an introductory level, *Am. J. Phys.* **70** 3.
3. M. Wittmann, R. Steinberg, and E. Redish (2002). Investigating student understanding of quantum physics: Spontaneous models of conductivity, *Am. J. Phys.* **70**, 218.
4. C. Singh (2001). Student understanding of quantum mechanics, *Am. J. Phys.*, **69**, 885-895.

5. D. Domert, C. Linder, A. Ingerman, (2005). Probability as conceptual hurdle to understanding one-dimensional quantum scattering and tunneling, *Euro. J. Phys.* **26**, 47-59.
6. C. Singh, M. Belloni and W. Christian (2006). Improving student's understanding of quantum mechanics, *Physics Today*, **8**, 43-49, August.
7. M. Malgieri, P. Onorato and A. De Ambrosis (2014). Teaching quantum physics by the sum over paths approach and GeoGebra simulation, *Euro. J. Phys.* **35**, 055024 (1-21).
8. C. Singh (2007). Helping Students Learn Quantum Mechanics for Quantum Computing, Proceedings of the Phys. Ed. Res. Conference, Syracuse, NY, AIP, (L. McCullough, P. Heron, L. Hsu Eds.), AIP Conf. Proc., Melville New York 883, 42-45.
9. A. Kohnle et al., (2014). A new introductory quantum mechanics curriculum, *Euro J. Phys.* **35**, 015001.
10. A. Kohnle et al., (2010). Developing and evaluating animations for teaching quantum mechanics concepts, *Euro. J. Phys.* **31**, 1441-1455.
11. C. Singh (2008). Student Understanding of Quantum Mechanics at the Beginning of Graduate Instruction, *Am. J. Phys.*, **76**(3), 277-287.
12. A. J. Mason and C. Singh (2010). Do advanced students learn from their mistakes without explicit intervention? *Am. J. Phys.* **78**(7), 760-767.
13. S. Y. Lin and C. Singh (2010). Categorization of quantum mechanics problems by professors and students, *Euro. J. Phys.* **31**, 57-68.
14. G. Zhu and C. Singh (2012). Surveying students' understanding of quantum mechanics in one spatial dimension, *Am. J. Phys.*, **80**(3), 252-259.
15. C. Singh (2008). Interactive Learning Tutorials on Quantum Mechanics, *Am. J. Phys.*, **76**(4), 400-405.
16. G. Zhu and C. Singh (2011). Improving students' understanding of quantum mechanics via Stern-Gerlach experiment *Am. J. Phys* **79**(5), 499-507.
17. G. Zhu and C. Singh (2012). Improving students' understanding of quantum measurement I: Investigation of difficulties, *Phys. Rev. ST PER*, **8**(1), 010117 (1-8).
18. G. Zhu and C. Singh (2012). Improving students' understanding of quantum measurement II: Development of Research-based learning tools, *Phys. Rev. ST PER*, **8**(1), 010118 (1-13).
19. G. Zhu and C. Singh (2013). Improving students' understanding of the addition of angular momentum in quantum mechanics, *Phys. Rev. ST PER*, **9**(1), 010101 (1-12).
20. E. Marshman and C. Singh (2015). Framework for understanding student difficulties in quantum mechanics, *Phys. Rev. ST PER* (in publication).
- C. Singh and E. Marshman (2015). Review of student difficulties in quantum mechanics *Phys. Rev. ST PER* (in publication).
21. C. H. Bennett and G. Brassard (1984). Quantum Cryptography: Public key distribution and coin tossing. in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 175.
22. C. Bennett (1992). Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Lett.* **68**, 3121-3124.
23. C. H. Bennett, G. Brassard and N. D. Mermin (1992). Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.* **68**(5), 557-559.
24. I. Gerhardt, et al. (2011). Full-field implementation of a perfect eavesdropper on a quantum cryptography system, *Nature Communications* **2**, 1.
25. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin (1992). Experimental quantum cryptography, *Journal of Cryptology* **5** (1), 3-28.
26. G. Brassard and L. Salvail (1993) Secret key reconciliation by public discussion *Advances in Cryptology: Euro crypt 93 Proc.* 410-423.
27. R. Hughes and J. Nordholt (2011). Refining quantum cryptography *Science* **333** (6049): 1584–1586.
28. A. Kohnle "Quantum Cryptography", QuVis: The University of St Andrews Quantum Mechanics Visualisation project. University of St Andrews, <http://www.st-andrews.ac.uk/physics/quvis>. See http://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-b92/B92_photons.html
29. <http://www.idquantique.com/>
30. R. Alleaume (2007). SECOQC White Paper on quantum key distribution and cryptography, *SECOQC*, 3-4.
31. W. K. Wootters and W. H. Zurek (1982) A single quantum cannot be cloned, *Nature* **299**, 802-803.
32. The entire QKD QuILT is available on the QuILTbeta website on COMPADRE <http://www.opensourcephysics.org/items/detail.cfm?ID=13514>
33. L. McDermott and the Physics Education Group at the University of Washington. (1996). Physics by Inquiry, Vols. I and II. John Wiley & Sons Inc., New York, NY.

34. M. Chi (1994). "Thinking Aloud." in *The Think Aloud Method: A Practical Guide to Modeling Cognitive Processes*, edited by M. W. Van Someren, Y. F. Barnard, and J. A. C. Sandberg Academic, London.