Weissman et al. *EPJ Quantum Technology* (2024) 11:64
https://doi.org/10.1140/epjqt/s40507-024-00276-4

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

Keep it secret, keep it safe: teaching quantum key distribution in high school

Efraim Yehuda Weissman[1*], Avraham Merzel[2], Nadav Katz[2] and Igal Galili[2]

*Correspondence:
efy.wei@gmail.com
[1]Jerusalem College of Technology, Jerusalem, Israel
Full list of author information is available at the end of the article

Abstract

Quantum Key Distribution (QKD) is a cryptography protocol based on the fundamental principles of quantum physics (QP). Teaching this subject does not require extensive knowledge beyond these principles, making it suitable for inclusion in high school (HS) curricula. Despite its relevance, teaching QKD in HS is yet understudied. In this study, we collected responses from 12th-grade students from various schools that adopted and applied the Discipline-Culture vision of the physics curriculum. We assessed their understanding through conceptual and quantitative problems and examined their attitudes regarding the motivation to study this subject. We analyzed the responses using content analysis, identifying the challenges and affordances of teaching QKD. The challenges faced by students have been categorized into three themes: difficulties with QP, difficulties with the QKD protocol, and difficulties with the mathematics involved in this context. Despite these challenges, we found that teaching QKD reinforces students' conceptual understanding of QP concepts and problem-solving skills. This work enhances educators' ability to address the challenges of teaching QP and suggests that teaching QKD in HS strengthens students' motivation to study QP.

Keywords: Quantum key distribution; High School Physics Education; Dirac Notation; Student Motivation

1 Introduction

In recent years, significant research and pedagogical efforts have focused on developing quantum physics (QP) curricula and studying their effects [e.g., 16, 22, 35, 37]. These efforts span quantitative [30] to phenomenological approaches [e.g., 17], and vary in their focus on quantum principles versus phenomena [44]. Some emphasize phenomena like interference [e.g., 41] and tunnelling [e.g., 17], while others focus on principles such as superposition [e.g., 32, 43], quantum state [e.g., 26], uncertainty [28], and wave function collapse [e.g., 8]. In these approaches, phenomena illustrate the principles.

The Discipline-Culture (DC) approach [11, 36, 42] similarly uses phenomena to illustrate QP principles. This three-folded approach defines the *nucleus* as the core principles, the *body* as consisting of phenomena derived from these principles, and the *periphery* as encompassing alternative understandings, such as concepts from other theories (e.g., classical physics when teaching QP) or misconceptions. Teaching using this approach is

Springer

deductive, centered on defining the principles, while employing phenomena to illustrate them and contrasting them with alternative concepts.

Given that QP underpins modern technology, teaching it effectively in high school (HS) is challenging, particularly with quantum technology. It is crucial to show that QP has real-world applications beyond being a philosophical theory [29]. However, the advanced knowledge required often leads to it being simplified into a "black box" that obscures understanding [1].

A significant technological application of QP is quantum key distribution (QKD), which is sometimes referred to as 'quantum cryptography' in the QP education literature. This topic represents a cutting-edge area of research and technological advancement, showcasing the practicality and relevance of QP in everyday life. Surveys with various expert populations stress that QKD is an important topic to teach for students, is essential for future workforce, relatively easier than other technological topics, and might foster motivation for learning QP [2, 10, 12–15]. Moreover, understanding the concepts of QKD requires minimal additional background beyond the basic principles of QP [9], making it relatively straightforward to teach in HS. Furthermore, teaching QKD can serve as a practical demonstration ('*body*') of the core principles ('*nucleus*') of QP, thereby reinforcing students' understanding of these fundamental concepts. DeVore and Singh [3] highlight the value of this approach, noting, 'This real-world application makes QKD a particularly useful vehicle for helping students learn about the fundamentals of quantum mechanics in an undergraduate course' (p. 1). Additionally, mastery of this topic can serve as an indicator of students' comprehension levels.

In this paper, we present a study on the instruction of the BB84 QKD protocol [33], which is designed to generate an encryption key of any desired length. This key, if used as a one-time key pad, is highly immunized against deciphering [18]. Since the protocol is well-known, we summarize it briefly here, as it is implemented with polarized photons, although other implementations are possible [e.g., 6].

The QKD protocol entails one party ('Alice') sending photons to another party ('Bob'), with each photon's polarization measured in one of two sets of axes (basis): horizontal-vertical ('+') or diagonal (45 degrees from the first set of axes; '×'), randomly selected for each photon. Bob performs measurements in the same manner. They then compare the measurement bases without disclosing the measurements' outcomes. For photons measured by both parties using the same basis, they can deduce that they obtained identical results, allowing them to establish a code known only to them. In the event of eavesdropping (by 'Eve'), the wave function collapses, resulting in changes to some of Bob's measurement outcomes. Alice and Bob can compare part of their results made in the same basis, and see if there is an eavesdropper.

The QKD protocol relies on the quantum nature of polarization and is grounded in principles such as superposition, Heisenberg principle, measurement, collapse of the wave function, and the probabilistic nature of measurement results. Furthermore, teaching this subject can incorporate a quantitative approach, which helps in understanding [30] and self-efficacy [6, 44], involving probability calculations. These calculations can range from straightforward scenarios with two equal probabilities to more complicated situations. Hence, QKD can be taught at various levels of quantitative complexity, tailored to the class level or available resources. Additionally, it is possible to integrate calculations based on Dirac notation. In addition, QKD can be used as an introduction to more intricate

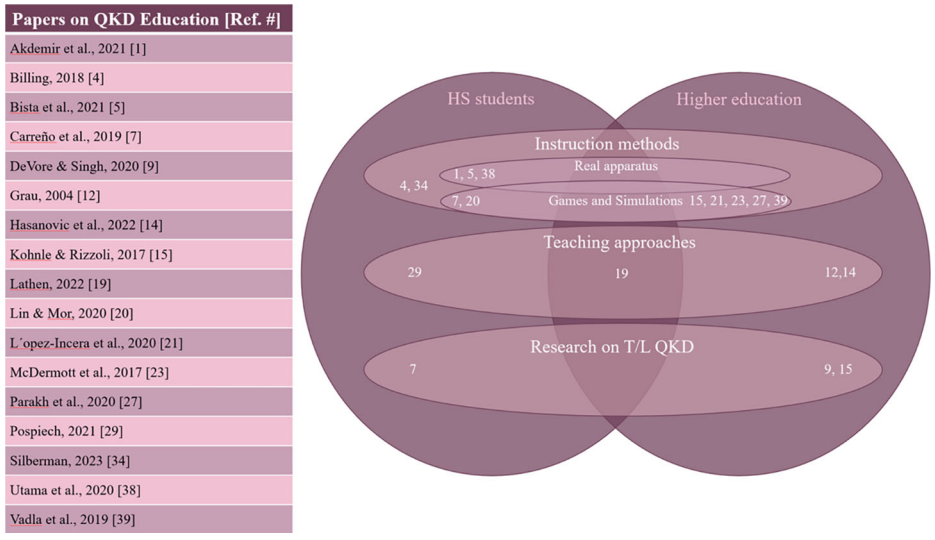


Figure 1 Organizing literature about teaching and learning (T/L) QKD

teaching units in quantum computing [31], and teaching QKD can have a positive effect on student motivation [1, 2, 7, 12].

The literature of teaching and learning QKD in the last 20 years is three-fold. The first type is proposals for instruction methods, mainly for higher education, but also for HS and the general public. Some of them include using real apparatus and some rely on games or simulations. Some of these include evaluation questionnaires that aim at assessing students' satisfaction with the proposed method. The second type is consolidating QKD in approaches for teaching, and the third type is research studies on teaching and learning QKD as a subject, trying to characterize its affordances and challenges (see Fig. 1). As Fig. 1 shows, there is a lack of studies attending research on secondary school population.

These considerations give rise to the following research questions:

(1) What are the affordances and challenges of teaching QKD in high school?

(2) What is students' motivation toward the subject, as observed in this study unit?

2 Method

2.1 Population and data collection

This study focused on high school students majoring in algebra-based physics. The sample comprised three 12th-grade classes (final year of studies) taught by two teachers in two different schools over three years. The students attending these classes were not sorted, and are considered standard physics students. Some of them excel in physics throughout HS while others are challenged by the subject matter. Throughout their studies and at the conclusion of the course, students filled various tasks and underwent tests and exams. We chose these tasks as representing students' knowledge about the core principles of QP and their ability to implement quantitative skills in problem solving, including transfer to unfamiliar systems. The interpretation of the questions and the issues they addressed were validated through discussion among the researchers and the teachers. One class (N = 13) answered questions 1-4, while two classes (N = 32) answered question 5. These assessments varied across different years and classes, according to the teachers' choices

and pedagogical considerations, thus differing in content and in the number of students addressing them. The findings are presented with the corresponding number of students who filled the tasks (see Table 1). The questions corresponding to QKD are provided in the Appendix, along with proposed full solution, for readers' convenience.

Two classes (N = 26) completed a reflection questionnaire aimed at exploring students' sentiments regarding the curriculum, with a focus on their motivation and opinions regarding QKD. We asked students to rate the importance of teaching QKD on a Likert scale of 1-6, and to explain their ratings.

2.2 Analysis

We analyzed students' answers using content analysis [cf. 40] to identify difficulties and misconceptions. Specifically, we meticulously examined each answer, tracking students' reasoning. We followed students' open answers and calculations step by step, and whenever an answer was incorrect, we attributed it to a specific difficulty that appeared to be the underlying cause. Additionally, we employed content analysis on the reflection questionnaires in order to identify their attitudes towards learning QKD.

The first stage of the analysis involved the first author inductively categorizing the students' responses and characterizing their difficulties. Next, the second author and a research assistant were presented with the students' responses and, based on the established categorization, were asked to provide their own categorizations. In the final step, the three sets of categorizations were compared. We discussed disagreements and adjusted the delineation of difficulties until full agreement was achieved among the researchers. A similar approach was employed in the analysis of the open-ended questions in the reflection questionnaires, in addition to calculating students' mean rating.

2.3 Educational context

Although QP is not part of the mandatory curriculum in the country of research, it was included in these classes by their teacher choice. Teachers chose to teach it by the DC approach. The total time allocated for teaching QP in these classes was approximately 30 hours, of them, about 75 minutes were dedicated to frontal teaching of QKD. Teaching QKD as an application is typically placed towards the end of the QP curriculum to illustrate the principles students have learned. The choice of the BB84 protocol is due to its relative simplicity, and proficiency in this protocol lays the foundation for understanding other protocols [9]. Prior topics to QKD were 'wavity' in its quantum meaning as a superposition with a probabilistic interpretation (including interference of the wave function); Heisenberg principle (not necessarily of position and momentum, but also, for example, of spin and polarization in different axes); the collapse of the wave function; interference, and entanglement. According to the DC approach, these principles and QKD were contrasted with alternatives from classical physics, such as classical cryptography. The teachers, of whom their classes participated in the study, also adopted a quantitative teaching approach [30], therefore they taught Dirac notation at a basic level. Therefore, students were able to deal with problems that require calculation of probabilities. In addition to teachers' lectures, teaching QKD included many forms of active learning: designated worksheets, video-based activities, simulations, and tours to university labs and to a commercial company specializing in developing cutting-edge QKD solutions (although, neither by BB84 protocol nor by polarization).

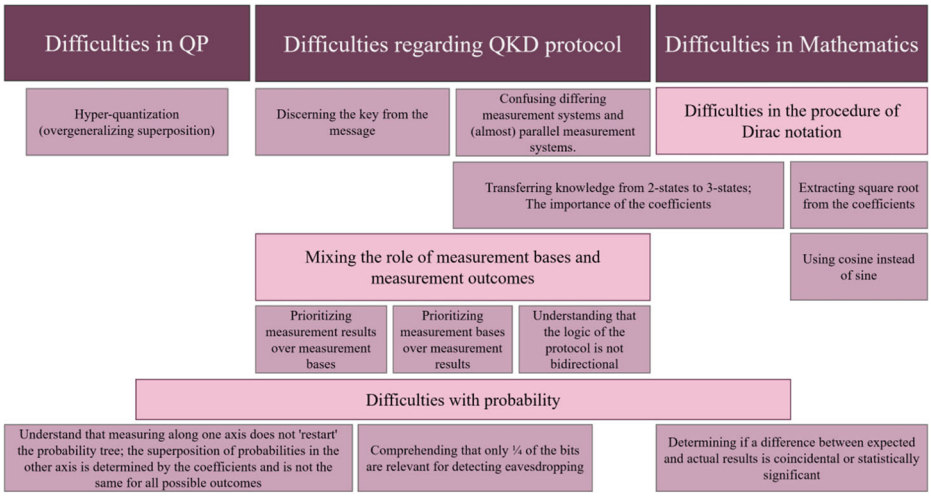


Figure 2 Themes of challenges while learning QKD

3 Findings

Through an examination of students' responses to quantitative and conceptual questions, we identified challenges and affordances that teaching QKD can engender. We disregard unsuccessful solutions due to occasional calculation mistakes or overlooking details while reading the questions, which are common challenges encountered by students at all levels in all physics fields. First, we report on students' challenges; then, we summarize the advantages of teaching QKD, including motivational aspects.

3.1 Challenges

We inductively organize the challenges we found into three major themes: Difficulties in QP, Difficulties regarding the QKD protocol, and Difficulties in relevant mathematics (see Fig. 2). Some challenges overlap between themes, and as such, we placed them at the intersection of themes. Notably, we found that difficulties related to aspects of probability permeate all themes. To represent this, we included a title spanning all theme columns in the model (see Fig. 2), indicating the overarching influence of probability across the themes. In the following subsections, we elucidate and provide examples of the various challenges within each theme. We added double parentheses for better readability and square parentheses for in-quotes explanations.

3.1.1 Difficulties in QP

This theme pertains to difficulties rooted in misunderstandings of QP aspects, with no direct connection to the QKD protocol. We did not find many difficulties exclusively related to this theme, as the questions were primarily focused on QKD. However, one difficulty that did emerge is 'hyper-quantization'. *Hyper-quantization* occurs when students (or teachers) overgeneralize and incorrectly attribute quantum behavior where it is not applicable [25]. This tendency usually arises during the learning process when learners have not fully grasped the subject matter. An example of this emerged in response to Q2a (see the Appendix), where students were asked to determine the presence of eavesdropping based on the list of bits presented to them. One student commented:

> *Kfir: "Because the deviation is less than a quarter, there is no reason to suspect eavesdropping; rather, it is likely due to the probabilistic superposition of the photon."*

This student identified only one of the two mismatching cases. Nonetheless, saying "*the probabilistic superposition of the photon*" suggests a belief that a photon is always in superposition, even when the wave-function has collapsed.

3.1.2 Difficulties regarding QKD protocol

Unsurprisingly, this theme is the largest category of challenges identified. It includes the categories of Discerning the key from the message, Confusing differing and parallel measurement systems, Mixing the role of measurement bases and measurement outcomes, which includes three sub-categories, and one category that is also part of the theme of Difficulties with quantum mathematics.

a) *Discerning the key from the message*: One of the challenges in QKD is understanding the necessity of filtering the bits. Students who have not internalized the concept of creating a key may mistake the sequence of bits for the key itself. Consequently, they might select all the bits. For example, in Q2b (see the Appendix), we encountered a student who considered all the bits as the key.

b) *Confusing differing measurement systems and* (*almost*) *parallel measurement systems*: Students with this difficulty would treat systems as distinct while disregarding differences between them that are too small to be expected if they were truly dissimilar. For example, in response to Q3b (see the Appendix) one student wrote:

> *Ariel: "There is a* $P = 0.5$ *to go [=the wave function would collapse] into each axis.*
> $P = (\cos 45^\circ)^2 = 0.5$
> *Here it will be 0.49 due to the deviation ((of 2%)), therefore*
> $P = (\cos\theta)^2 = 0.49$
> $\theta = 45.573^\circ \rightarrow$ *deviation of* 0.573°*"*

This student subtracts 2% (0.01) when the systems are tilted in 45 degrees respectively, instead of reducing 2% of parallel measurement systems, as indicated by the minor discrepancies in the outcomes.

c) *Mixing the role in the protocol of measurement bases and measurement outcomes:* Under this category we found three difficulties.

i) *Prioritizing measurement results over measurement bases*: Difficulty in identifying the critical aspect of the measurement basis in the protocol, can lead to challenges in distinguishing the key among all the transmitted bits. For instance, students may focus solely on the binary outcomes (0, 1) received by both parties, regardless of the measurement basis. This difficulty may lead them to include bits where the same outcome was obtained (e.g., Alice and Bob obtained '1') and consider them part of the key, even if Alice measured in basis × and Bob in basis +. For example, in Q2b, where students were asked to extract the key from a given set of photons, we identified two students experiencing such difficulty. They constructed a key comprising more bits than those measured in the same basis (13 bits). Both students derived their key from matching outcomes rather than matching bases. This misconception of prioritizing outcomes over measurement bases represents the challenge to understand the importance of measuring in the same basis for Alice and Bob. We found indications of the same

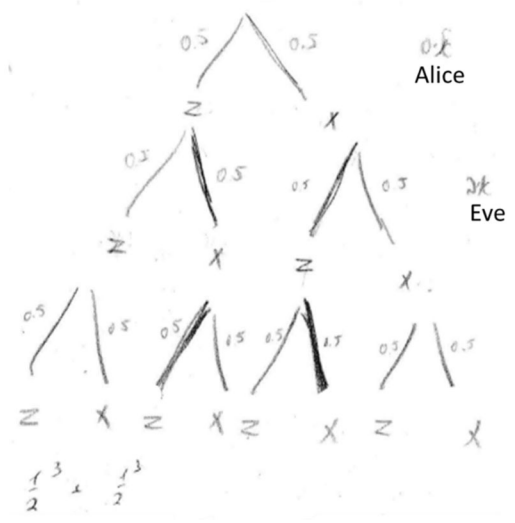


Figure 3 Example for student constructing probability tree considering only the measurement bases

misconception in Q5a (see the Appendix), given to students who did not answer Q2. In Q5a, two students associated bases and measurement outcomes asserting mistakenly that when the results are the same, the bases are the same, and conversely, when the results of Alice and Bob differ, the bases are different.

ii) *Prioritizing measurement bases over measurement results*: Underestimating the importance of the probability of obtaining each outcome in a measurement, and failing to understand that this probability depends on previous results and the superposition states, might lead students to focus solely on measurement bases in multi-stage measurements such as QKD. We identified such difficulties in Q5b (see the Appendix), in which students were asked to calculate the probability of a certain event in a spin 1 system. Nine students (out of 32) constructed their probability trees using the measurement bases (x, z) instead of considering the probabilities of the measurement results. Among these students, two built trees that exclusively utilized the measurement bases. For example, the tree drawn by Shiri (Fig. 3):

The other seven did include the results at the last stage of the measurements, but they assigned equal probabilities to each outcome rather than considering the coefficients denoted in the question (see difficulties in understanding probability below). This difficulty could also be viewed through the prism of classical probability and quantum probability: choosing the measurement basis can be made randomly in various ways, including classical methods (e.g., flipping a coin), while the outcomes are determined by quantum inherent probability. Mixing these (incorrectly) in the probability tree might suggest that students did not fully understand the distinction between these two types of probabilities.

iii) *Understanding that the logic of the protocol is not bidirectional*: if the bases Alice and Bob use are the same (no eavesdropping, no noise), it necessarily means the results of the measurements are the same. However, if the results are the same, it does not necessarily mean the bases they use are the same. This difficulty may be similar to the previous one, as it also requires an understanding of the importance

of comparing bases in the protocol, but it demands a deeper comprehension of the protocol itself. For instance, in Q5a five students (out of 32) concluded from similar measurement results that Alice and Bob necessarily measured in the same basis rather than acknowledging that this given data is not informative enough.

3.1.3 Difficulties in mathematics (with regard to QKD), and specifically, in the use of Dirac notation

Teaching QKD with DN often reveals students' struggles with mathematical concepts. This section highlights specific difficulties students encountered, underscoring the cognitive challenges of learning advanced QP in HS.

Extracting square root from the coefficients and Using cosine instead of sine: Some teachers adopted our recommendations to incorporate quantitative teaching of QP and to utilize Dirac notation for problem-solving. In spite of the advantages this approach entails (see 'Affordances', below), we observed students encountering difficulties with the mathematical applications. For instance, in Q3b, two students failed to correctly extract the square root from the coefficients, while another struggled to identify the appropriate basis for calculation, mistakenly using cosine instead of sine.

Transferring knowledge from two-states QKD protocol to three-states QKD protocol; The importance of the coefficients: During the lessons, students mainly encountered the two-state protocol. Generalizing to a three-states protocol is not trivial. Students experiencing this difficulty tend to assign a 0.5 probability to each possible outcome in the protocol. Similar to the difficulty of understanding that the probability is determined by the coefficients in the state representation, they tend to "restart" the probability in each measurement in a probability tree. An example of this difficulty is expressed in the words of one of the students who responded to question Q5c (see the Appendix):

> *Yarden: Initially Alice measured in basis x and obtained zero. After that, Eve has measured on a different basis, so she again has a 50% chance of obtaining zero or one.*

In Yarden's expression of "*she again has a 50% chance of obtaining zero or one"* he expresses his view of the situation as a two-state system.

We observed two students experiencing this difficulty in Q4a (see the Appendix) and two students in Q5c (different students, as those who answered Q4 did not answer Q5). Note, that if Alice obtained zero, Eve could not have obtained zero. This difficulty intersects the themes of QKD protocol and mathematics. In our sample, students facing such difficulty manage well with other questions that require calculations utilizing Dirac notation. However, it appears that either the three-state QKD protocol overloads them cognitively, or relying on the familiar two-state protocol erroneously simplifies the problem.

3.1.4 Difficulties with probability

In this sub-theme of challenges, focusing specifically on the probabilistic nature, we found three difficulties: i) Comprehending that only 1/4 of the bits are relevant for detecting eavesdropping, which is a difficulty in understanding the QKD protocol; ii) Understanding that measurement in a different axis changes the state in the previous axis to superposition, but does not "restart" the probability tree and does not mean all possible outcomes have the same probability, which is a difficulty that combines understanding QP and the protocol; and iii) Determining if a difference between expected and actual results is coincidental or statistically significant, which is a mathematical difficulty.

i. *Probability and QKD protocol: Comprehending that only 1/4 of the bits are relevant for detecting eavesdropping*: Understanding that the only relevant bits are those which Alice and Bob measured in the same basis and Eve measured in the other basis (e.g., Alice: x, Eve: z, Bob: x) is a prerequisite for solving probability problems in QKD. Constructing a probability tree is not required since multiplying the probability of Bob choosing the same basis as Alice (0.5) with the probability of Eve choosing the opposite basis (0.5) is sufficient. However, working on question Q5b, seven (out of 32) students built probability trees with branches representing the measurement bases to acknowledge this. Only after achieving this understanding did they further calculate probabilities related to the measurement outcomes.
ii. *Probability and the combination of QP and QKD protocol: Understanding that measuring along one axis does not 'restart' the probability tree; the superposition of probabilities in the other axis is determined by the coefficients and varies among different possible outcomes*: We observed a difficulty that seems to stem from the additional cognitive load encountered when the QKD protocol is applied to QP concepts. Students who generally understand QP principles might struggle with QKD problems, erroneously believing that each measurement 'restarts' the probabilities equally for all outcomes. For instance, in Q4a, two students incorrectly asserted that the probability of obtaining zero when measuring spin along the other axis was 0.5 because it "reverts to the probability of the first basis" (Ron). Notably, both students provided states in Dirac notation but disregarded the coefficients. However, these two students did not ignore the coefficients when solving problems that used Dirac notation but were unrelated to QKD (which we report elsewhere). This suggests that the context of QKD introduces an additional layer of complexity for some students. These observations lend weight to our claim that the difficulty encountered is not merely a misunderstanding of QP.

Six other students claimed in response to Q4b that each measurement in a different axis 'restarts everything', including the probability of obtaining a specific state. They did not realize they should consider the probability of obtaining a specific state according to previous measurements. Further evidence of this misunderstanding we found in responses to Q5c, which is similar to Q4a. Seventeen students demonstrated this unripe understanding, suggesting that each measurement in a different axis reconstructs the superposition on the perpendicular axis, thereby re-enabling *all* possibilities (−1, 0, 1), as in the following quote:

> *Oron: Alice measured zero on the x-axis, Eve eavesdropped on the z-axis and found zero => the former measurement collapsed and therefore there is again superposition of the three states, and Eve measured zero. After that, Bob measured on the x-axis and also found zero (he measured in a different axis; therefore, the previous measurement collapsed and there is again a superposition of the 3 states).*

The (mis)understanding that measuring in a different axis restarts the probability tree can lead to the notion that each state has the same probability. For example, among the 17 responses mentioned previously, five students explicitly emphasized that the probability of obtaining each result is similar (0.33). Note that while measurement in one axis does place the spin in another axis in superposition, the

results of consecutive measurements depend on the results of the previous measurement. Assuming an equal probability distribution after a measurement indicates a lack of coherent conceptual understanding. Even interpreting the coefficients as the square root of the probability does not align with the idea of reinstating all possible outcomes. For instance, when Alice measured along the x-axis and obtained zero, and then Eve measured along the z-axis, the notion that a superposition entails re-establishing *all* possible outcomes would suggest that Eve could obtain *any* of the possible outcomes (z^+, z^0, z^-). However, squaring the coefficients shows a 0 probability of obtaining z^0, leading to a contradiction.

We observed a combination of this difficulty with the one previously mentioned, which involves prioritizing measurement bases over measurement results, in Q5b. Seven students constructed probability trees where the initial branches represented the measurement bases and the final branch assumed equal probabilities, rather than reflecting the actual coefficients. This can be seen in the example below, depicted in the probability tree drawn by Avera, where each branch at the bottom junction is assigned a probability of 1/3 (see Fig. 4).

A different interpretation of these results might be akin to the concept of hyper-quantization mentioned earlier, where a complete 'restart' is applied with every change of the measurement axis. This suggests that students are treating superposition as overarching across several measurements.

Similarly, in a multi-stage measurement question (Q4a, Q4b, Q5b, Q5c), before measuring along the z-axis, the system is no longer in a superposition state along the x-axis since the wave function has collapsed along this axis. Since the question does not specify the outcome along the x-axis, there are three possible outcomes: x^+, x^0 or x^-. These become "classical" options, meaning the wave function has collapsed to one of these states (and not a superposition of these states). Measuring along the z-axis then requires taking into account the (now classic) probability of obtaining

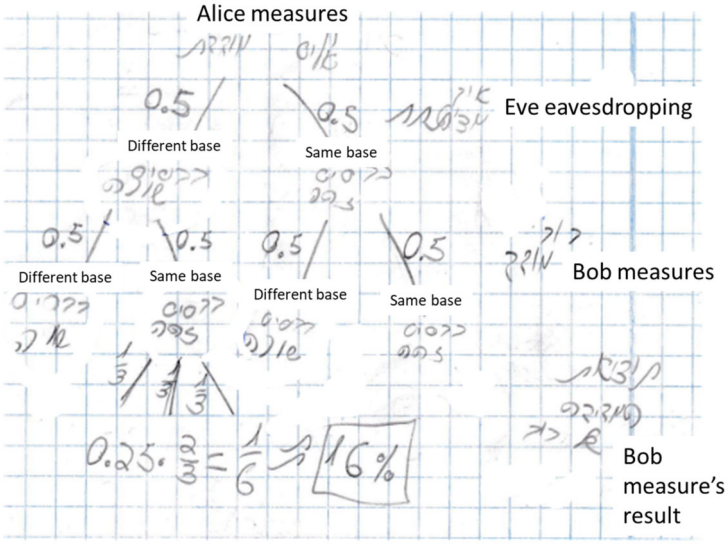


Figure 4 Example for a student constructing a probability tree, with the initial branches representing the measurement bases and the final branch showing a probability of $\frac{1}{3}$. (Translation to English is included)

either result. Students who adopt a hyper-quantization perspective on 'measurement' may view these probabilities as quantum probabilities, hence believing that the measurement causes the wave function to collapse (again) in an overarching manner, causing the system to "forget everything". Such an understanding would lead them to assign the same probability to all possible outcomes, regardless of the coefficients presented in the state description.

iii. *Probability and mathematics: Determining if a difference between expected and actual results is coincidental or statistically significant:* This difficulty directly relates to students' understandable (in HS) lack of knowledge in statistics. Students facing this difficulty tend to resolve this dilemma, which should be addressed with statistical tools, by relying on intuition. For example, in Q2a, students were asked to decide whether eavesdropping occurred, using the evidence of 2 out of 13 bits, made in the same measurement basis, that resulted in different outcomes. Expecting to affect the outcomes at a 0.25 ratio, students anticipated approximately 3 measures to be misaligned. Lacking proper tools to differentiate between 2/13 from 3/13 (or from 3.25/13), nine students (out of thirteen) indicated possible eavesdropping, albeit not aligning precisely with theoretical expectations, and four argued against eavesdropping, citing the lower-than-expected number of deviations. Alternatively, students may have assumed—perhaps influenced by instructions—that results should be statistically representative, and any deviations likely stem from some noise in the measurement system rather than eavesdropping. One student expressed this interpretation as follows:

> *Ariel: Eavesdropping would be expressed in about* 1/8 *different results. Less than* 1/12 *[he refers to 2 measures out of 25:* 2/25 < 1/12*] are different ('different' ((means)) - same basis, different result; that is, someone measured in the other axis [=basis] and caused a new superposition in the axis that is supposed to be polarized in the same axis [=basis]. For example: -,- and now it would be -,/), hence we can assume that no one is eavesdropping, and these are random mistakes*.

Note that posing such questions should facilitate in-class discussions about the probabilistic nature of QP and QKD, rather than being used to grade students' achievements.

3.2 Affordances

Albeit the aforementioned difficulties, teaching QKD in HS bears many affordances. Summary of the number of students answered correctly (or had only minor mistakes), including the main theme of each question, is shown in Table 1.

In the following sections we portray the affordances in three themes, based on the DC framework mentioned in the introduction: 1) Understanding the *nucleus* of QP; 2) Experimenting the *body* through understanding implementation of QP; and 3) Acquiring the students with quantitative skills of problem solving in QKD context.

3.2.1 Understanding the nucleus of QP

One of the most important benefits of teaching QKD in HS is the solid internalization of the basic principles of QP. For example, Q1 (see the Appendix) was designed to assess

Table 1 Number of students who answered each question correctly and the main theme of each question

Question	Understanding QP *nucleus*	Implementing QP *body*	Quantitative skills of problem solving in QKD context	Number of students answered correctly out of (number of students received the question)
Q1	•			13/(13)
Q2a	•	•		13/(13)
Q2b		•		10/(13)
Q3a	•	•		13/(13)
Q3b			•	10/(13)
Q4a		•	•	10/(13)
Q4b	•	•	•	6/(13)
Q5a	•	•		24/(32)
Q5b	•	•	•	7/(32)
Q5c	•	•	•	6/(32)

students' understanding of the basic principles of the QKD protocol, and specifically their recognition that a photon measured in one basis exists in a superposition in another basis. Answering this question requires understanding fundamental QP principles, serving as a gauge of the students' comprehension and their ability to use these principles to create explanations for phenomena in their own words. All students who responded to this question provided correct explanations grounded in core principles. Each student referenced at least one fundamental principle, with 10 (out of 13) students mentioning superposition, six citing Heisenberg's uncertainty, and five discussing the collapse of the wave function. For example:

> *Hadar: "The polarization of the photon is in an eigenstate in the + basis and is therefore in* ***superposition*** *in the × basis according to the* ***uncertainty principle****. When the photon reaches the × polarizer, the polarization will* ***collapse*** *into one of two conflicting possibilities: \ or /."*

Hadar's explanation, which utilizes the principles of superposition, Heisenberg's uncertainty, and the collapse of the wave function in a measurement, exemplifies how learning QKD can serve as a practical means for students to demonstrate their understanding of QP principles.

We found further evidence of this foundational understanding in more complicated QKD scenarios. In Q5a, for example, students adeptly applied their understanding of the collapse of the wave function and Heisenberg's uncertainty principle with a system of spin-1. Impressively, 31 out of 32 students accurately determined the outcomes in scenarios where the bases of measurement were the same, affirming the consistency of results due to the wave function collapse. Conversely, in cases where the measurement bases differed, 24 students successfully recognized the inherent uncertainty, correctly asserting that Bob's results could not be definitively known. Such proficiency suggests that QKD teaching may contribute to solidify students' theoretical knowledge, reinforcing the *nucleus* against the *periphery* of QP.

Other questions require students to understand the *nucleus* of QP; therefore, these questions are also denoted in the first column of Table 1.

3.2.2 Implementing the body of QP

In the teaching and learning unit about QKD protocol, students struggled to understand how QP principles are implemented in a specific technological application. Hence, it is

worth examining how students understand the features of this application. This understanding involves identifying the relevant bits for the key and the key itself, and determining whether eavesdropping had occurred reflecting their understanding of the ratio of misaligned outcomes that indicate eavesdropping. These understandings were tested with a limited number of measurements (in Q2a and Q2b) and with a large number of photons with a small (2%) discrepancy rate of the photons measured in the same basis (in Q3a).

Except for three, all students (n = 13) successfully identified the relevant measurements and could extract the key. Moreover, all but one student correctly explained that in the case of eavesdropping, unmatching outcomes should occur in a quarter of the photons measured in the same basis; although interpretations of these results varied among them, as previously described in the passage dealing with difficulties in probability and mathematics. Additionally, they all correctly recognized when the percentage of errors was significantly lower than expected in cases of eavesdropping, leading them to conclude that eavesdropping was unlikely.

Students' understanding can be acknowledged if they successfully transfer their knowledge to unseen scenarios. In Q4 and Q5, students were asked to apply their knowledge by extending their understanding of two-state quantum systems to a more complex three-state scenario (spin-1 system). The probabilities were no longer fixed at 0.5, and the measurements were taken in alternating bases. This task required them to exhibit their proficiency in interpreting representations of quantum states by inferring probabilities from the coefficients and clearly displaying their comprehension of what is measured and the possible outcomes, thus actualizing the '*body*' of QP through QKD protocol.

Specifically, students were expected to recognize that in the given system, a spin zero along one axis contains no component of spin zero along the other axis (see Q4a in the Appendix), ultimately resulting in a 0 probability for obtaining a spin zero when measured along one axis, after measuring zero in the perpendicular axis. Furthermore, students needed to grasp the complexity of quantum measurements and state collapse in the system: on the one hand, each measurement leads to the collapse of the wave function along the measured axis, and the particle 'forgets' its previous state along any perpendicular axis and is in a superposition state in that axis. On the other hand, the possible outcomes of the measurement are influenced by the state that existed prior to the measurement. This introduces a layer of complexity beyond the simpler scenario of two states with probabilities of 0.5 each (see Q4b and Q5b-c in the Appendix). Additionally, students were required to calculate probabilities using a 'probability tree', a method most students had not previously encountered in their coursework.

Many students successfully transferred their understanding from a two-state scenario to a three-state scenario with probabilities other than 0.5 (see Table 1). Most students correctly identified the relationship between states on different axes in Q4a and concluded that there is a 0 probability of obtaining spin zero. Additionally, although not in the majority, quite a few students demonstrated an understanding of the effects of eavesdropping: six out of thirteen in Q4b, by analyzing measurements in alternating bases; and six out of thirty-two in Q5c, by correctly determining that the presented outcomes were not possible, as spin zero states do not contain components of spin zero along other axes. Furthermore, five other students regarded Q5c as dealing with the probability of detecting eavesdropping (Shuvu: *"impossible, since Alice and Bob measured in the same basis and*

obtained the same result"), thus, responding correctly to the question according to their interpretation.

3.2.3 Acquiring students with quantitative problem-solving skills in the QKD context

Integrating mathematical structures in HS QP education is crucial for fundamental, pedagogical, cognitive and motivational reasons [30]. Teaching QKD to HS students highlights the advantages of equipping students with the ability to solve quantitative problems. Specifically, this includes representing quantum states with Dirac notation (DN) and manipulating them to reach solutions.

Moreover, students were not intimidated by DN formalism; they demonstrated an understanding of representing quantum states with DN, and many could transfer their knowledge to a three-state system described in this formalism (e.g., Q4a and Q4b), as mentioned above (see Table 1). Among these students, five performed calculations using DN to verify the probabilities, with one providing a verbal interpretation alongside the calculation result. Common to several questions (Q1, Q3b, Q4a, Q5c) is that answering them does not require calculations with DN. Nevertheless, many students used DN as a means to solve these problems (three students in Q1; ten in Q3b; five in Q4a; nine in Q5c). These findings suggest that DN serves as a useful tool for simplifying quantitative problems, instilling confidence in students to represent quantum states and quantum ideas, and confront related challenges.

Another impressive finding is that ten (out of thirteen) students were able to calculate the angle of deviation between Alice's and Bob's systems (Q3b), assuming that the differences stemmed from this discrepancy (although three of them had minor mistakes, as discussed previously, hence, they did not reach the correct answer). They demonstrated computational proficiency, relying on previously encountered formulas or, alternatively, the use of DN.

However, quantitative reasoning was not confined to DN, as the problems posed by teachers to their students involved other mathematical skills, such as constructing probability trees. Students demonstrated their ability to infer quantitatively the probability of eavesdropping in a three-state QKD system in Q5b. Seven students calculated the correct probability for eavesdropping according to probability trees. Of them, two provided fully correct responses, four calculated the complement probability, and one had a minor calculation mistake.

3.2.4 Motivation

One of the affordances of teaching QKD in HS is that it instills motivation. In a reflection questionnaire administered to two classes (N = 26), students were asked to rate the importance of learning QKD on a Likert scale from 1 to 6 and to explain their rating in an open-ended question. The mean score was 3.96 (SD = 1.48), indicating generally positive attitudes toward the subject. Most students (85%) described the topic as interesting, and most (77%) emphasized its practical relevance to everyday life. For example:

> *Oron: "QKD is an interesting topic in my opinion and very relevant to our everyday life. It is also a relatively simple topic to learn, so I think it is an advantage ((to learn it in class))."*

Four students expressed excessive enthusiasm, using slang terms like 'cool' to emphasize their interest. When examining students' perspectives on QKD as a means to demonstrate

QP, four claimed that it did not help them understand QP, and another four stated this topic is not important or too difficult to understand. However, two students mentioned that it aided in understanding the Heisenberg principle, and three noted that it helped them better understand the theory of QP.

4 Discussion

Quantum Key Distribution (QKD) is an important topic in Quantum Physics (QP), especially for the future workforce [10, 12–14], with everyday implications [9, 12]. This study addresses the gap in QP education research concerning the teaching of QKD in high schools (HS) and gathered responses from quizzes and final tests of three HS classes taught by two different teachers over the last several years under the Discipline-Culture (DC) framework. These teachers incorporated the QKD protocol, such as BB84, into their curricula with a quantitative approach. Although similar, not all classes had identical teaching methods and activities (e.g., visiting a QKD company). However, we believe that this variability is part of the strength of this topic: QKD can be taught in various ways and still likely achieve success, at least to some extent. Being aware of the challenges students might face will further pave the way for successful teaching.

4.1 QKD challenges

We meticulously analyzed these responses, seeking insights into students' challenges and affordances. We identified three main themes of challenges: Difficulties with QP, Difficulties with the QKD protocol, and Difficulties in Mathematics related to QKD. Some sub-themes, such as Difficulties with probability, permeated more than one theme.

By applying this thematic categorization of difficulties on the findings of DeVore and Singh [3], we can add another brick to the growing tower of understanding students' difficulties with QKD. Their development of a tutorial for learning QKD for upper-level undergraduate students revealed several difficulties with QP, particularly with polarization, which support the claim that teaching QKD effectively tests students' understanding of QP concepts. They also encountered challenges with the protocol, specifically with probability, transferring from polarization to spin, and understanding how a bit is extracted in the protocol. In addition to these types of difficulties, our study identified challenges with understanding sequences of bits and the construction of the key.

Some difficulties related to the QKD protocol, such as discerning the key from the message and prioritizing measurement bases over measurement results, have been described in the literature for undergraduate students [9] but not in HS students.

4.2 QKD affordances

Despite these challenges, students managed to grasp many aspects of the subject, including solving quantitative problems, and found learning QKD motivating, as it was both interesting and practical for everyday life. In exploring the pedagogical applications of QKD, it becomes clear that it serves not only as a teaching tool but also as a conceptual bridge. Professionals in the field view QKD as a potent illustration for the key quantum concepts of entanglement, Heisenberg's principle, and no-cloning [24]. This perspective aligns with Carreño et al. [7], who demonstrated that teaching QKD helps students understand concepts such as projective measurements, indistinguishability of pathways, coherent superpositions, entanglement, and Bell tests. Our findings complement these insights

by showing that QKD effectively exemplifies key quantum principles like superposition, Heisenberg principle, and the collapse of the wave function in a high school classroom setting.

4.3 Adjusting the level of teaching: quantitative vs. conceptual teaching

The increasing demand for skills related to algorithms for quantum information and communication underscores the importance of early exposure to QP. Fox et al. [10] highlight in their survey that these skills are highly valued by commercial industry companies. They point out that due to the unintuitive nature of QP, it is beneficial for students in higher education to become acquainted with these concepts as early as possible. Building on this idea, we advocate for introducing QKD even earlier, during HS education.

QKD can be seamlessly integrated into the HS curriculum, offering various depths of engagement. While some suggest that BB84 is too complicated for students without prior knowledge (for example, [19]; who offers another protocol and programming implementation to overcome this difficulty), others argue that teaching QKD in HS should be more conceptual than quantitative [e.g., 1]. Nonetheless, our findings indicate that by learning QKD with a quantitative approach, involving Dirac notation and probability trees, students can manage to overcome much of the intricacy and even solve quantitative problems, while simultaneously gaining a conceptual understanding. However, tailoring the subject to different mathematical proficiency levels among students should be considered. For instance, teaching can range from basic probability calculations, such as 50-50 scenarios, to more complicated mathematical frameworks involving probability trees or Dirac notation. Adjusting the level of teaching must be navigated carefully, as our findings suggest an increase in student difficulty as the mathematical complexity of the questions rises. This flexibility ensures that QKD is accessible to a wide range of students, accommodating different backgrounds and levels of mathematical skills.

Thus, a structured teaching path that begins with introducing the BB84 protocol, progresses to the EK91 protocol, and subsequently develops the concept of entanglement in high school, appears to be feasible [9, 29]. This topic in QP can also be connected to quantum computing, even without complex numbers, but maintaining a mathematical approach [e.g., 4].

The question of "what should we teach in QP in HS" should always be kept open, with various QP education researchers pushing the boundaries of what is possible and beneficial for students to learn at this level. Our study challenges the borders of contemporary curricula by asserting that teaching QKD protocols quantitatively is relevant in addressing quantum technological subjects and plausible in the sense that students understand most of it and succeed in quantitative problem-solving.

4.4 Motivational aspects of teaching QKD

QKD has the potential to motivate students to learn QP [1]. It "positively impacts the interest of students in physics and promotes an appreciation of the role of quantum mechanics in modern industry" [7, p. 10], and it also appeals to engineering students [2]. Consistent with these findings, our study reveals that most HS students recognize the importance and relevance of this topic to their everyday lives and future careers and find it interesting. Although some students did not find it engaging or helpful in learning QP concepts, others emphasized that it aided their understanding of such concepts. Our results suggest

that early exposure to QKD can enhance student interest and preparedness for advanced studies in quantum technologies.

4.5 Conclusion

Teaching QKD offers a nuanced blend of conceptual understanding, problem-solving skills, and motivational engagement. It not only demystifies quantum principles but also actively engages students in cutting-edge technology, enhancing their conceptual comprehension and problem-solving skills. This study contributes to the growing body of literature advocating for the early introduction of quantum technologies in secondary school education.

This research has demonstrated the efficacy of a deductive teaching approach to QKD, utilizing it as a '*body*' to exemplify the '*nucleus*', contrasted with the '*periphery*' of QP. The students succeed to grasp the new knowledge while not drowned in the formalism of the considered phenomena. This method has proven beneficial in reinforcing students' understanding and application of core quantum concepts. However, the potential of an inductive teaching approach, where QKD is used as a gateway to introduce and explore basic QP principles, also presents a viable alternative [29].

Given the significant role QKD can play in educating about quantum principles and technologies, it is imperative to develop and refine instruments that both examine and assess students' knowledge and difficulties, such as those we have presented. These instruments, along with our findings, are likely applicable not only in HS setting but also in higher education.

Future studies should explore teaching additional QKD protocols and investigate effective teaching materials and methods that address student challenges. Such research will further push the boundaries of what is feasible in QP education at the HS level, preparing students for advanced studies and careers in quantum technologies.

Appendix

Q1

Alice sends a stream of photons to Bob (described from left to right in the table). '+' is a horizontal/vertical measurement basis. '-' and '|' are horizontal and vertical measurement outcomes, respectively. We define '-' = 0, '|' = 1. '×' is a measurement basis at 45 degrees. '/' = 1 and '\' = 0 are measurement outcomes at 45 degrees and 135 degrees, respectively.

A photon is measured by Alice in the horizontal/vertical basis ('+') and found to have vertical polarization ('|'). Explain physically what will happen if Bob measures it in the diagonal basis ('×'). Address the possible outcomes and explain them physically.

Solution: When the photon is measured by Alice in the + basis, its wave function collapses to the '|' state. The + and × bases are in Heisenberg uncertainty relations, so if the photon is in the vertical polarization eigenstate, it is in a superposition of right-diagonal and left-diagonal states. If Bob measures it in the × basis, the photon will collapse with a

0.5 probability to either of them and return to being in a superposition with respect to the + basis.

	1	2	3	4	5	6	7	8	9	10	11	12	$\frac{1}{3}$	14	15	16	17	18	19	20	21	22	23	24	25
Alice's basis	×	×	+	×	+	+	+	×	+	×	+	×	×	×	+	+	+	×	+	×	+	+	+	×	×
The bit Alice sent	\	/	|	/	-	|	|	\	-	\	-	\	\	/	|	|	-	/	|	/	-	|	-	/	/
Bob's basis	+	×	+	+	+	+	×	+	×	×	+	+	+	×	×	+	+	+	+	×	×	×	+	+	×
Bob's result	-	/	|	-	-	-	/	-	\	\	-	-	|	\	/	|	-	-	|	/	/	\	-	|	/

Q2a

Refer to the table of measurements above. Is anyone eavesdropping? If so, provide evidence. If not, explain what the table would look like in case someone was eavesdropping. Assume that even though the number of photons is not large, if there was eavesdropping, you would be able to detect it.

Q2b

Find the key that will be received (including the error if there was eavesdropping).

Solution (for parts a and b): According to the Table, 13 bits were measured in identical bases. The incorrect bits are bits 6 and 14.

If someone was eavesdropping, we would expect a quarter of the bits measured in identical bases to be incorrect. In this case, 2 bits certainly increase the suspicion of (at least partial) eavesdropping, but it is not certain.

Q3a

In another case, many photons were sent. Alice and Bob checked their systems and found that 2% of the bits in which they chose the same measurement bases did not match. They were sure that there was no eavesdropping and that the error was caused by Bob's coordinate system not being properly calibrated. Explain what the percentage of non-matching bits should be in case of eavesdropping and explain why they were sure there was no eavesdropping.

Solution: Half of the photons were measured by Alice and Bob in the same basis, and half in different bases. That is, the photons of interest to them are half of all the photons sent. Of those photons, if Eve is indeed eavesdropping, then in half of them, she measures in the same basis as Alice and Bob, so she does not affect them. Only in the other half, where she measures in a different basis, does she cause the wave function to collapse into her basis and to become in superposition in Alice and Bob's basis. When Bob measures these, in half he receives the same result as Alice, and in half, he will receive a different result from Alice. In total, in the case of eavesdropping, in a quarter of the relevant photons (one-eighth of all the photons sent), Alice and Bob will be able to see Eve's traces. 2% is much less than one-eighth (12.5%) of the photons sent.

Q3b

What was the angular deviation of Bob's measuring system relative to Alice's?

Solution: If Bob measures in a coordinate system that is tilted relative to his system, then his measurements in the horizontal state can be expressed as: $|\theta\rangle = cos\,\theta\ \ |x\rangle + sin\,\theta\ \ |y\rangle$. If we want to examine the probability that Alice indeed had the vertical state, i.e., the $|y\rangle$ state, we need to calculate the overlap of $\langle y \mid \theta\rangle$. From the data given, we know that the probability of receiving an incorrect bit is 0.02 (2%). Therefore: $\left|\langle y \mid \theta\rangle\right|^2 = 0.02$. Hence:

$$\cos\theta\,\langle y \mid x\rangle + \sin\theta\,\langle y \mid y\rangle = \sin\theta$$

$$\sin^2\theta = 0.02 \rightarrow \sin\theta = 0.1414$$

$$\theta = 8.13^\circ$$

Q4

Reminder: We discussed the spin of an electron. An electron has a spin magnitude of $\frac{\hbar}{2}$, therefore, in any axis we choose, we can only obtain spin values (i.e., the magnitude of the component along the measured axis) of $\pm\frac{\hbar}{2}$. There are particles in nature with a spin magnitude of $\hbar$, therefore, in any axis we choose, we can obtain one of the following values: $-\hbar$, 0, $\hbar$. In quantum physics, many quantized quantities take on discrete values, including spin which can only take on values in increments of $\hbar$. We denote $|z^-\rangle, |z^0\rangle, |z^+\rangle$ as the states where the spin along the z axis has values of $-\hbar$, 0, $\hbar$ respectively. These states are, of course, mutually exclusive.

It is possible to express the spin states of such a particle along the x-axis as:

$$|x^-\rangle = \frac{1}{2}|z^-\rangle - \frac{1}{\sqrt{2}}|z^0\rangle + \frac{1}{2}|z^+\rangle$$
$$|x^0\rangle = \frac{1}{\sqrt{2}}|z^-\rangle - \frac{1}{\sqrt{2}}|z^+\rangle$$
$$|x^+\rangle = \frac{1}{2}|z^-\rangle + \frac{1}{\sqrt{2}}|z^0\rangle + \frac{1}{2}|z^+\rangle$$

And from here we can obtain:

$$|z^-\rangle = \frac{1}{2}|x^-\rangle + \frac{1}{\sqrt{2}}|x^0\rangle + \frac{1}{2}|x^+\rangle$$
$$|z^0\rangle = -\frac{1}{\sqrt{2}}|x^-\rangle + \frac{1}{\sqrt{2}}|x^+\rangle$$
$$|z^+\rangle = \frac{1}{2}|x^-\rangle - \frac{1}{\sqrt{2}}|x^0\rangle + \frac{1}{2}|x^+\rangle$$

We will apply the BB84 protocol on spins of such particles (this is obviously not BB84 but a similar protocol).

Q4a

Alice sends a particle to Bob. Before that, she measured and found that its spin along the x-axis is zero. Bob measures the spin of the particle along the z-axis. What is the probability that he will obtain spin zero in that axis? Explain your answer.

Solution: A spin state of zero along the z-axis is a state that is not composed of the zero spin state of the x-axis, and therefore the probability is 0.

Q4b

Now there are two eavesdroppers: Eve and Carol. Alice measured along the x-axis and obtained spin zero. Eve measured along the z-axis, Carol measured along the x-axis, and Bob along the z-axis. What is the probability that Bob will obtain spin zero?

Solution: A zero state along any axis has a 0 probability of obtaining zero along the perpendicular axis, and a 0.5 probability of obtaining positive or negative. A positive or negative state has a 0.25 probability of obtaining positive or negative along the perpendicular axis, and a 0.5 probability of obtaining zero in it. It is easier to describe it this way: a zero state along one axis has a 0 probability of obtaining a zero spin along the perpendicular axis and a 1 probability of obtaining a non-zero spin. A non-zero state has a 0.5 probability of obtaining zero along the perpendicular axis, and a 0.5 probability of obtaining a non-zero value.

Therefore, when Alice sends a particle with spin zero along the x-axis, Eve will certainly obtain a non-zero spin along the z-axis. Carol has a 0.5 probability of obtaining a spin zero along the x-axis, and then Bob cannot obtain a spin zero along the z-axis. Carol has a 0.5 probability of obtaining a non-zero spin along the x-axis, and then Bob has a 0.5 probability of obtaining zero along the z-axis, i.e., a probability of 0.25.

Q5

Reminder: We talked about the spin of an electron. The electron has a spin of magnitude $\frac{\hbar}{2}$, therefore in any selected axis we can obtain a spin value (that is, the size of the component in the measured axis) only from the $\frac{\hbar}{2}$ values. There are particles in nature that have a spin value of $\hbar$, therefore in any chosen axis we can obtain one of the following values: $-\hbar$,0, $\hbar$. In quantum physics, many physical quantities receive discrete values. In general, the spin can only receive values multiplication of $\hbar$. We denote $|z^-\rangle, |z^0\rangle, |z^+\rangle$ as the states where the spin along the z axis has values of $-\hbar$, 0, $\hbar$ respectively. These states are, of course, mutually exclusive.

The spin x states of such a particle can be expressed as follows:

$$|x^-\rangle = \frac{1}{2}|z^-\rangle - \frac{1}{\sqrt{2}}|z^0\rangle + \frac{1}{2}|z^+\rangle$$
$$|x^0\rangle = \frac{1}{\sqrt{2}}|z^-\rangle - \frac{1}{\sqrt{2}}|z^+\rangle$$
$$|x^+\rangle = \frac{1}{2}|z^-\rangle + \frac{1}{\sqrt{2}}|z^0\rangle + \frac{1}{2}|z^+\rangle$$

So, one can obtain:

$$|z^-\rangle = \frac{1}{2}|x^-\rangle + \frac{1}{\sqrt{2}}|x^0\rangle + \frac{1}{2}|x^+\rangle$$
$$|z^0\rangle = -\frac{1}{\sqrt{2}}|x^-\rangle + \frac{1}{\sqrt{2}}|x^+\rangle$$
$$|z^+\rangle = \frac{1}{2}|x^-\rangle - \frac{1}{\sqrt{2}}|x^0\rangle + \frac{1}{2}|x^+\rangle$$

We will apply the BB84 protocol to the spins of such particles (it is of course not BB84 but a procedure similar to it). Alice launches a particle bob. For each particle she measures the spin along either the x-axis or the z-axis. She writes to herself the value obtained from each particle (−1, 0, or 1). Bob also measures the particles. Their selection of the basis of measurement for each particle is random, and Bob does not know which basis Alice measured. Before Alice made the measurements it is assumed that z spin states come with equal probabilities, as well as x spin states.

Q5a

Complete the following table. Where the answer is not known with certainty, mark "?".

	1	2	3	4	5	6	7	8	9
Alice's basis	x	x	z	x	z	z	x	z	x
Alice's result	1	-1	0	0	0	-1	1	0	-1
Bob's basis	x	z	x	x	z				
Bob's result						0	1	-1	1

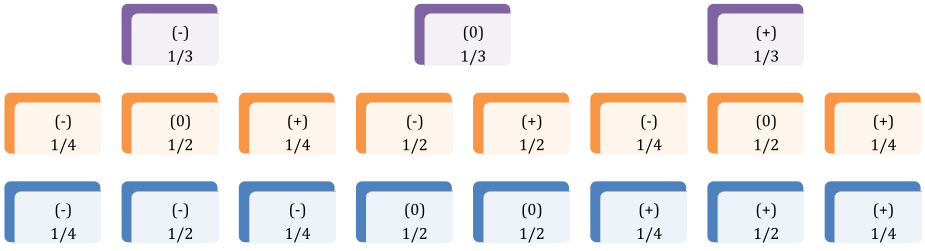
Solution:

	1	2	3	4	5	6	7	8	9
Alice's basis	x	x	z	x	z	z	x	z	x
Alice's result	1	-1	0	0	0	-1	1	0	-1
Bob's basis	x	z	x	x	z	**x**	**?**	**x**	**z**
Bob's result	**1**	**?**	**?**	**0**	**0**	0	1	-1	1

Q5b

In the case that Eve is eavesdropping, what will be (approximately) the ratio of measurements (out of all the particles that were launched) in which there will be traces of Eve's activity (that is, Bob will obtain a different result than Alice's, even though they measure on the same basis)? Note that the calculation here is slightly more complicated than the case of BB84.

Solution:



Purple - Alice's measurement Orange - Eve's measurement Blue - Bob's measurement

In this probability tree only the matching measurements are presented, since it is easier to calculate. That is: $\frac{1}{3}\left(\frac{1}{4}\cdot\frac{1}{4}+\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{4}\cdot\frac{1}{4}\right)+\frac{1}{3}\left(\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}\right)+\frac{1}{3}\left(\frac{1}{4}\cdot\frac{1}{4}+\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{4}\cdot\frac{1}{4}\right)=\frac{1}{3}\left(6/16+\frac{1}{2}+6/16\right)=\frac{1}{3}\cdot 20/16=5/12$. Hence, the mismatching probability is 7/12. This is for only the relevant bits, so from all the bits sent it is 7/12* 1/4 = 0.146

Q5c

Alice measured a certain particle along the x-axis and found that its spin is zero. Then Eve measured it along the z-axis and found that its spin was zero, finally Bob measured its spin along the x-axis and found it to be zero. Describe what happened in each step of measurement, taking into account the quantum aspects at each step. If the said description is not possible - explain why.

Solution: As one can see from the description of states at the beginning of the question, if there is a zero spin state on one axis, there is a 0 probability of obtaining zero spin on the other axis. Therefore, the description is not possible.

List of abbreviations

DC, Discipline culture; DN, Dirac notation; HS, High school; QKD, Quantum key distribution; QP, Quantum physics.

Author contributions
EY.W. and A.M. designed the learning materials, collected the data, wrote the main manuscript, and conducted the analysis and validation. All authors conceptualized the research. N.K. and I.G. reviewed the manuscript and provided feedback.

Funding
Not applicable

Data Availability
The supporting data for this study is not publicly available. However, upon reasonable request, the corresponding author can provide access to the supporting data to reserchers for verification and replication purpose. Note: the data is in Hebrew. Requests for access to the supporting data should be directed to Efy Weissman at efy.wei@gmail.com .

Declarations

Ethics approval and consent to participate
The data was collected following the approval of the Institutional Ethics Committee and with the consent of the students, their parents, and teachers to use the learning and teaching materials anonymously.

Consent for publication
Not applicable

Competing interests
The authors declare no competing interests.

Author details
[1] Jerusalem College of Technology, Jerusalem, Israel. [2] The Hebrew University of Jerusalem, Jerusalem, Israel.

Received: 17 June 2024 Accepted: 20 September 2024 Published online: 03 October 2024

References

1. Akdemir Z, Menekse M, Hosseini M, Nandi A, Furuya K. Introducing quantum key distribution to high school students. Sci Teach. 2021;88:44–51.
2. Baily C, Finkelstein ND. Teaching quantum interpretations: revisiting the goals and practices of introductory quantum physics courses. Phys Rev Phys Educ Res. 2015;11(2):020124. https://doi.org/10.1103/physrevstper.11.020124.
3. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11. https://doi.org/10.1016/j.tcs.2014.05.025.
4. Billig Y. Quantum computing for high school students. Qubit Publishing; 2018.
5. Bista A, Sharma B, Galvez EJ. A demonstration of quantum key distribution with entangled photons for the undergraduate laboratory. Am J Phys. 2021;89(1):111–20. https://doi.org/10.1119/10.0002169.
6. Bøe M, Henriksen EK, Angell C. Actual versus implied physics students: how students from traditional physics classrooms related to an innovative approach to quantum physics. Sci Educ. 2018;102(4):649–67. https://doi.org/10.1002/sce.21339.
7. Carreño MJ, Sepúlveda J, Tecpan S, Hernández C, Herrera F. An instrument-free demonstration of quantum key distribution for high-school students. Phys Educ. 2019;54(6):065006. https://doi.org/10.1088/1361-6552/ab377c.
8. Chiofalo ML, Foti C, Michelini M, Santi L, Stefanel A. Games for teaching/learning quantum mechanics: a pilot study with high-school students. Educ Sci. 2022;12(7):446. https://doi.org/10.3390/educsci12070446.
9. DeVore S, Singh C. Interactive learning tutorial on quantum key distribution. Phys Rev Phys Educ Res. 2020;16(1):010126. https://doi.org/10.1103/physrevphyseducres.16.010126.
10. Fox MFJ, Zwickl BM, Lewandowski HJ. Preparing for the quantum revolution: what is the role of higher education? Phys Rev Phys Educ Res. 2020;16(2):020131. https://doi.org/10.1103/physrevphyseducres.16.020131.
11. Goorney S, Foti C, Santi L, Sherson J, Yago Malo J, Chiofalo ML. Culturo-scientific storytelling. Educ Sci. 2022;12(7):474. https://doi.org/10.3390/educsci12070474.
12. Grau BC. How to teach basic quantum mechanics to computer scientists and electrical engineers. IEEE Trans Ed. 2004;47(2):220–6. https://doi.org/10.1109/te.2004.825215.
13. Greinert F, Müller R, Bitzenbauer P, Ubben MS, Weber K-A. The future quantum workforce: Competences, requirements and forecasts arXiv:2208.08249 (2022).
14. Hasanovic M, Panayiotou C, Silberman D, Stimers P, Merzbacher C. Quantum technician skills and competencies for the emerging Quantum 2.0 industry. Opt Eng. 2022;61(08):081803. https://doi.org/10.1117/1.oe.61.8.081803.
15. Kohnle A, Rizzoli A. Interactive simulations for quantum key distribution. Eur J Phys. 2017;38(3):035403. https://doi.org/10.1088/1361-6404/aa62c8.
16. Krijtenburg-Lewerissa K, Pol HJ, Brinkman A, van Joolingen WR. Insights into teaching quantum mechanics in secondary and lower undergraduate education. Phys Rev Phys Educ Res. 2017;13(1):010109. https://doi.org/10.1103/physrevphyseducres.13.010109.
17. Krijtenburg-Lewerissa K, Pol HJ, Brinkman A, van Joolingen WR. Secondary school students' misunderstandings of potential wells and tunneling. Phys Rev Phys Educ Res. 2020;16(1):010132. https://doi.org/10.1103/physrevphyseducres.16.010132.
18. Kumar P, Prabhakar A. Quantum key distribution using spin wave–optical interactions. IEEE J Quantum Electron. 2010;46(11):1542–8. https://doi.org/10.1109/jqe.2010.2052914.
19. Lethen T. Bit commitment as an introduction to quantum cryptography. Eur J Phys. 2022;43(5):055402. https://doi.org/10.1088/1361-6404/ac78a7.

20. Lin J, Mor T. Quantum candies and quantum cryptography. In: Theory and practice of natural computing. Cham: Springer; 2020. p. 69–81.
21. López-Incera A, Hartmann A, Dür W. Encrypt me! A game-based approach to Bell inequalities and quantum cryptography. Eur J Phys. 2020;41(6):065702. https://doi.org/10.1088/1361-6404/ab9a67.
22. Lovisetti L, Organtini G, Giliberti M. Inducing the construction of formal axioms of quantum mechanics and fostering their comprehension by high school students: the effectiveness of a conceptual approach. Il Nuovo Cimento C. 2023;46(6):1–24.
23. Mcdermott S, Vadla S, Bommanapally V, Parakh A, Subramaniam M, Ostler E. Teaching quantum cryptography using a virtual 3D educator: QuaSim. QuaSim National Cyber Summit. 2017.
24. Merzel A, Bitzenbauer P, Krijtenburg-Lewerissa K, Stadermann K, Andreotti E, Anttila D, et al. The core of secondary level quantum education: a multi-stakeholder perspective. EPJ Quantum Technol. 2024;11(1):27. https://doi.org/10.1140/epjqt/s40507-024-00237-x.
25. Merzel A, Weissman EY, Katz N, Galili I. Toward teacher training for teaching quantum physics in high school. In: Borg Marks J, Galea P, Gatt S, Sands D, editors. Physics teacher education. Challenges in physics education. Cham: Springer; 2022. p. 161–72. https://doi.org/10.1007/978-3-031-06193-6_12.
26. Michelini M, Ragazzon R, Santi L, Stefanel A. Discussion of a didactic proposal on quantum mechanics with secondary school students. Il Nuovo Cimento. 2004;27(5):555–67.
27. Parakh A, Bommanapally V, Chundi P, Subramaniam M. Quantum cryptography exercise schedules with concept dependencies. J Colloq Inf Syst Secur Educ. 2020;8:8.
28. Pospiech G. Uncertainty and complementarity: the heart of quantum physics. Phys Educ. 2000;35(6):393–9. https://doi.org/10.1088/0031-9120/35/6/303.
29. Pospiech G. Quantum cryptography as an approach for teaching quantum physics. Teaching-learning contemporary physics: from research to practice; 2021. p. 19–31.
30. Pospiech G, Merzel A, Zuccarini G, Weissman E, Katz N, Galili I, et al. The role of mathematics in teaching quantum physics at high school. In: Teaching-learning contemporary physics: from research to practice; 2021. p. 47–70. https://doi.org/10.1007/978-3-030-78720-2_4.
31. Satanassi S, Ercolessi E, Levrini O. Designing and implementing materials on quantum computing for secondary school students: the case of teleportation. Phys Rev Phys Educ Res. 2022;18(1):010122. https://doi.org/10.1103/physrevphyseducres.18.010122.
32. Seskir ZC, Goorney SR, Chiofalo ML. Educating to the "culture" of quantum technologies: a survey study on concepts for public awareness. Eur J STEM Educ. 2024;9(1):03. https://doi.org/10.20897/ejsteme/14193.
33. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett. 2000;85(2):441–4. https://doi.org/10.1103/PhysRevLett.85.441.
34. Silberman DM. Teaching quantum to high school students. In: Hagan DJ, McKee M, editors. Seventeenth conference on education and training in optics and photonics: ETOP 2023. Bellingham: SPIE; 2023.
35. Stadermann HKE, van den Berg E, Goedhart MJ. Analysis of secondary school quantum physics curricula of 15 different countries: different perspectives on a challenging topic. Phys Rev Phys Educ Res. 2019;15(1):010130. https://doi.org/10.1103/physrevphyseducres.15.010130.
36. Tseitlin M, Galili I. Physics teaching in the search for itself: from physics as a discipline to physics as a discipline-culture. Sci Educ. 2005;14:235–61.
37. Ubben MS, Veith JM, Merzel A, Bitzenbauer P. Quantum science in a nutshell: fostering students' functional understanding of models. Front Educ. 2023;8:1–14. https://doi.org/10.3389/feduc.2023.1192708.
38. Utama AN, Lee J, Seidler MA. A hands-on quantum cryptography workshop for pre-university students. Am J Phys. 2020;88(12):1094–102. https://doi.org/10.1119/10.0001895.
39. Vadla S, Parakh A, Chundi P, Quasim SM. A multi-dimensional quantum cryptography game for cyber security. J Colloq Inf Syst Secur Educ. 2019;6:19.
40. Vaismoradi M, Turunen H, Bondas T. Content analysis and thematic analysis: implications for conducting a qualitative descriptive study. Nurs Health Sci. 2013;15(3):398–405. https://doi.org/10.1111/nhs.12048.
41. van den Berg E, van Rossum A, Grijsen J, Pol H, van der Veen J. Teaching particle-wave duality with double-slit single-photon interference in Dutch secondary schools. In: Research and innovation in physics education: two sides of the same coin. Cham: Springer; 2020. p. 135–43.
42. Weissman EY, Merzel A, Katz N, Galili I. Teaching quantum mechanics in high-school–discipline-culture approach. J Phys Conf Ser. 2019;1287:012003 Bristol: IOP Publishing. https://doi.org/10.1088/1742-6596/1287/1/012003.
43. Weissman EY, Merzel A, Katz N, Galili I. Teaching quantum physics as a structured physics theory in high school. J Phys Conf Ser. 2021;1929(1):012051. https://doi.org/10.1088/1742-6596/1929/1/012051.
44. Weissman EY, Merzel A, Katz N, Galili I. Phenomena and principles: presenting quantum physics in a high school curriculum. Physics. 2022;4(4):1299–317. https://doi.org/10.3390/physics4040083.