LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
Department "Institut für Informatik"
Lehr- und Forschungseinheit Medieninformatik
Prof. Dr. Heinrich Hußmann

Bachelor-Thesis

Supporting the Understanding of Quantum Key Distribution Through Tangible User Interfaces

Linus Stetter
linus.stetter@campus.lmu.de

Bearbeitungszeitraum: 09.06.2022 bis 27.10.2022
Betreuerin: M.Sc. Sarah Delgado Rodriguez
Verantw. Hochschullehrer: Prof. Dr. Florian Alt

Zusammenfassung

Durch Quantencomputer sind bisher als sicher geglaubte IT-Sicherheitskonzepte womöglich bald veraltet. Ein besonders hohes Risiko besteht dabei für Verschlüsselungssysteme. Damit sind nicht nur unsere privaten Nachrichten in Gefahr, sondern auch sicherheitskritische öffentliche Infrastrukturen. Um diese Gefahr vorzubeugen, gilt es Quantencomputer sichere Verschlüsselungssysteme zu entwickeln, bevor unsere klassischen gebrochen werden. Neben neuen Entwicklungen von Verschlüsselungsalgorithmen und Sicherheitsprotokollen ist auch die Aufklärungsarbeit ein wichtiger Bestandteil, um diese Sicherheitslücke zu schließen. Nicht nur Fachkräfte, sondern auch die breitere Masse an Laien muss aufgeklärt werden, dass insgesamt die Popularität des Themas gesteigert wird. Ein geeigneter Themeneinstieg ist die Quantum Key Distribution (QKD). Um Laien QKD zu erklären haben wir eine Designidee für einen Tangible User Interface (TUI) Prototypen entwickelt. Mithilfe des TUIs soll unserer Zielgruppe das Thema QKD, anhand einer seiner Anwendungen dem BB84 Protokoll, zugänglich und verständlich gemacht werden. Für die Entwicklung der Designidee haben wir zuerst eine ausführliche Literaturrecherche über TUIs im Kontext von Wissensvermittlung betrieben. Wir haben TUIs in einem Design Space kategorisiert und herausgefunden, dass sie motivierend sind und den Einstieg in ein komplexes Thema erleichtern können. Zweitens haben wir auf Grundlage einer Umfrage ein Nutzungsszenario evaluiert, für welches das TUI am geeignetsten ist. Das TUI soll in einem externen Präsentationsszenario eingesetzt werden. Als drittes haben wir Experten zu einem Co-Design Workshop eingeladen mit dem Ziel, erste Designideen für ein TUI Prototypen zu gewinnen. Wir haben die insgesamt vier Designvorschläge diskutiert und diese dann als Inspiration für unseren finalen QKD-TUI-Prototyp Design Vorschlag genommen.

Abstract

Quantum computers may soon make IT security concepts previously thought to be secure obsolete. Encryption systems are at exceptionally high risk. Besides our private messages, security-critical public infrastructures are in danger. In order to prevent this threat, we need to develop quantum computer secure encryption systems before attackers break our current encryption system. In addition to new developments in encryption algorithms and security protocols, awareness is essential to closing this security gap. Besides domain experts, we need to educate the broader mass of laypeople to increase the overall popularity of the topic. A suitable entry point in this domain is Quantum Key Distribution (QKD). To explain QKD to non-experts, we have developed a design idea for a Tangible User Interface (TUI) prototype. With the TUI's help, the topic of QKD should be made accessible and understandable to our target group using one of its applications, the BB84 protocol. To develop the design idea, we first conducted extensive literature research on TUIs in the context of knowledge transfer. We categorized TUIs in a design space and found that they are motivating and can facilitate entry into a complex topic. Second, based on a survey, we evaluated a usage scenario for which the TUI is most suitable. The external presentation scenario suits best for a TUI. Third, we invited experts to a co-design workshop intending to gain initial design ideas for a TUI prototype. We discussed four design proposals and then used these as inspiration for our final QKD-TUI prototype design proposal.

Aufgabenstellung

Tangible User Interfaces (TUIs) are frequently applied in learning contexts, since they can convey complex information in an intuitive and engaging manner. Hence, we aim at investigating whether TUIs can support their users in understanding complex and abstract IT security concepts. In particular, we focus on non-experts' understanding of the still frequently unknown topic of Quantum Key Distribution (QKD). We conducted a online survey with 8 QKD-experts to gather first insights on when and how they usually explain aspects of QKD to other persons.
This thesis contributes to the research on usable security by deriving design concepts for a TUI that allows non-experts to understand the process of QKD based on the BB84 protocol. In particular, the project comprises the following steps:

- a literature review on TUIs in learning contexts and also teaching methods in relation to QKD and the BB84 protocol
- the identification of an appropriate usage scenario and target group for a TUI, based on the results of the previously conducted online survey
- the development and conduction of a co-design workshop with experts to derive possible design concepts for such a TUI
- the interpretation of the results of the co-design workshop and discussion of their implications for the development of future "TUIs for understanding QKD".

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbstständig angefertigt, alle Zitate als solche kenntlich gemacht sowie alle benutzten Quellen und Hilfsmittel angegeben habe.

München, 27. Oktober 2022

.....

Contents

CONTENTS

1 Introduction

Q-Day is the day when quantum computers succeed in cracking the public encryption system. This latter would put the fundamental infrastructures of our society at risk. We are talking about our energy supply, financial system, or military infrastructures [37]. A quantum computer needs 4098 stable qubits to break a 112-bit RSA encryption [73]. The IBM Eagle currently has the most stable qubits with 127, but IBM predicts that they could have a quantum computer with over 1000 stable qubits by 2023 [68]. Even then, we are only at just under a quarter of the qubits needed for breaking a weak RSA encryption. Hence, the goal is to develop new encryption schemes before quantum computers break our classical ones. The science of Post Quantum Cryptography is working toward just that. The first step of a quantum computer secure key exchange already exists. In 1984 Bennett and Brassard developed the BB84 protocol, a concrete application of Quantum Key Distribution (QKD) [5].

1.1 Motivation and Research Question

In addition to new developments in soft- and hardware, awareness and attention to the topic of QKD are also relevant, especially since there is the possibility that QKD will be part of future standard IT security concepts. Thereby we set our focus on explaining QKD to non-experts. Our goal is to find a way to offer a platform to the broad masses to inform themselves about this topic without requiring a solid background knowledge in computer science or physics. Based on a survey by Delgado Rodriguez et al., we have gained the first insights about the QKD explanations of eight QKD experts. From this survey, it appears that QKD is not easy to explain, and some of the explanation attempts are not sufficient. In addition, the experts also indicated which tools they currently use to explain QKD. Besides explanations without tools, mostly prefer pictures, slides, or texts. We conclude that these tools do not support the explanation enough. So the idea is to use a tool that is better suited to explain such a complex topic to non-experts.

Tangible User Interfaces (TUI) are a HCI technology that has been successfully used for transferring knowledge. Technology-enhanced learning with TUIs could be a solution to make QKD explanations understandable for non-experts. In the course of the thesis, we found that TUIs have the property to overcome entry barriers for a complex topic. Therefore, they seem to be suitable for our goal. In this thesis, we determine what types of TUIs researchers use in an educational domain and we create a design space and try to categorize TUIs.
To our knowledge, no TUI currently represents and/or explains QKD. So to implement such a TUI, we first need a suitable prototype.

Our research question is as follows: *How could a design for a TUI prototype look to explain QKD using the BB84 protocol?*

For this, we clarify that an external presentation scenario is most suitable for the TUI. We also define five key BB84 aspects (qubits, involved parties, bases/filter, measurement, public channel), which are fundamental for understanding.

1.2 Applied Methodology

To derive design ideas for our research question, we conducted a co-design workshop. This qualitative methodology is also theoretically possible with end users. However, since we first needed a design idea for a prototype, we decided to invite experts. They should be able to understand the BB84 protocol, and explain it through a TUI. For this purpose, we designed a questionnaire to evaluate the possible participants' previous knowledge and select them based on this knowledge. Our goal was to conduct the workshop with experts from different domains. We recruited five students, one research assistant with a computer science background, and three curators from the Deutsches Museum Munich with a physics background.
We structured the workshop in three steps. First, we provided information and background knowledge (step one) to prepare the participants for their creation session (step two). Finally, there was a short evaluation of the results in a feedback session (step three). We allowed the participants to decide at which level of detail they would like to propose a TUI prototype. Partly they exceeded our expectations by building small 3D models, which one can already categorize as a low-fidelity paper prototypes. With the help of the analyzed results of the workshop, we could finally develop a proposal for a QKD-TUI prototype ourselves.

1.3 Content Overview

Following this introduction, the thesis starts with background information. In the chapter 2, we clarify the background on HCI and Learning, explain TUIs, present the problem with classical cryptography, and introduce the QKD topic. Chapter 3 discusses a TUI design space. Here we categorized TUIs despite their diversity and showed the advantages and disadvantages of learning with TUIs. After that, in chapter 4, requirements for the QKD-TUI are defined. Here, in addition to a usage scenario, the essential aspects of the BB84 protocol are selected. In chapter 5, the study design, we clarify how our method was selected, describe the study procedure and content, and clarify how participants were selected. Chapter 6 presents the results of both the questionnaire and the co-design workshop. We discuss limitations and future work in chapter 7. In chapter 8 we discuss the results of the questionnaire and workshop. The last chapter 9 then presents the conclusion, in which we recapitulate the entire work and its results.

2 Background

In order to create a basic understanding from the beginning and prevent misunderstandings, the following section explains four central topics (i.e., research on learning in HCI, Tangible User Interfaces, the problem with classic cryptography, background QKD) while giving background knowledge additionally. It is common to encounter different terms with semantically similar meanings when one deals with the Tangible User Interfaces (TUI) research area. Therefore this section explains and creates the terminology that applies to this thesis.

2.1 Human Computer Interaction supported Learning

Human-Computer Interaction (HCI): Most computers, or machines in general, need a human to execute most tasks. Within HCI, the goal is to make the machine as functional and usable as possible [34]. The terms functionality and usability are fundamentally crucial for HCI. Functionality describes the set of functions the respective machine provides to achieve a specific goal. However, this is only of value if the usability is correspondingly high. Meaning the functions can be used efficiently and goal-oriented by the user. The balancing act between functionality and usability determines the effectiveness of a system [34].
Today teaching or simply explaining something without HCI is hard to imagine. If well integrated into the learning environment, computer-assisted teaching plays an important role in planning the lesson, presenting, and communicating with students [56, 49]. Technological learning-environment enrichment also helps "[develop] students' higher scientific processing skills" [2]. Kirschner et al. have shown that learning with and from computers enhances communication, strengthens the learning process, and trains problem-solving skills [38]. However, it is not only computers per se that increase student achievement. Applications can assist students with learning and also increase performance [56, 39, 42]. A significant advantage of learning applications is that they allow users to set their own pace. Of course, this could also disadvantage people with less discipline. The various ways such applications present learning content help students better absorb and structure content in their mind's eye [2]. However, to take advantage of these benefits, it is essential to be aware of the downsides of using too much technology in an educational context.
Technical problems can hold up instruction, especially when the staff is untrained in its use. Combining multiple technologies can make things worse. Suppose the effectiveness of the HCI design is low with poorly integrated technology. In that case, this increases the complexity and thus also the cognitive performance that one must encounter to guarantee the handling of several technologies and their interfaces [30]. In addition, technologies can distract learners and thus weaken students' concentration [35, 46].
In contrast to the downsides of a weaker concentration, Usun et al. have shown that students' motivation is enhanced when technology is combined with learning principles [62, 2]. Zzet et al. found in 2008 that computer-based education concepts are more effective than traditional methods [66]. It is important to note that through computer-based education concepts, students can understand concepts that are too complex for the current state of knowledge [67, 11, 31, 22]. This insight is vital in the further course of this work.
To close this subsection, we want to highlight two more unique features that HCI supported learning enables. First, working in groups helps students engage better with the learning material and develop a deeper understanding of the subject matter [17, 25]. Jeong et al. found in their meta-analysis that computer-supported collaborative learning promotes natural learning by using various technological and pedagogical strategies [30, 16, 61]. In addition, technology support for collaboration fosters cooperation, which helps strengthen the community, visualize complex concepts and ideas, and share information more effectively [29].
The second feature relates to attitude when working with technology in Computer Supported Education. It is well known that a positive attitude promotes learning, while a negative one hinders it

[2]. Another meta-analysis by Anil et al. concluded that computer-supported education has a moderate but significant positive effect on student attitudes [2]. Furthermore, teachers develop positive attitudes and more self-efficacy when using computers in learning environments [55]. Such an improvement in attitude is associated with higher expectations, better assumptions, stronger emotions, and improved beliefs [58, 40].

2.2 Tangible User Interface

Tangible User Interfaces (TUIs): Rather than any HCI technology, this bachelor thesis deals specifically with Tangible User Interfaces (TUIs). TUIs come in many forms and designs with different functionalities, so there is no concrete or universally applicable definition. A good approximation is given in the paper by Ishii et al. They talked about tangible bits, which try to bridge the gap between the physical and virtual world and make bits accessible and manipulable through physical objects [27]. The chapter 3 shows clearly how different TUIs can be, in which domain one can use them, and how.
In order to understand TUIs deeply, one cannot get around the concept of tangibles. As the term implies, a tangible is a touchable object. A TUI consists of an interactive and reactive part regarding the interaction [57]. Most commonly, the interactive part is tangible, and the reactive part is, for example, a built-in display that responds accordingly to user interaction, but not necessarily. Nevertheless, in the context of TUI, it is essential to mention that a tangible object has to interact with digital information, referring to Karola Marky's doctoral thesis [43]. A tangible object represents a so-called metaphor, which is used representatively in context, for example, to illustrate complex concepts or create an analogy for the user [41]. The metaphors can be strongly abstract or an exact representation of the representative object. Of course, whether the tangible ultimately is realistic or not is a design question. Essential is that the user has something to support they imagination or even to extend it in order to advance the learning process [41].
This supporting attribute is where TUIs are fascinating. When learning new, complex concepts, TUIs have three significant advantages over other HCI technologies [10, 47]. First, participants' attitude toward TUI technology, especially compared to traditional learning methods (including computers), is overwhelmingly positive. Secondly, TUIs are very well suited to develop a User-Interface (UI) that works collaboratively. Classic TableTop-TUIs would be an example of tangible objects as inputs with a responsive display. The advantages of collaborative learning do not necessarily result from the TUI itself, but it is an optimal platform for it, respective to other HCI technology [10, 47]. As a final advantage, third,TUIs ideally make topics that are too difficult for the learners' current level of knowledge nevertheless understandable [13, 52]. Other HCI technologies may have the same advantage, but the explorative and intuitive way of dealing with a TUI is what makes it special [44].

2.3 The Problem with Classic Cryptography

From the HCI and TUI background, it is clear that through technology-enhanced learning, complex concepts can be understood better and with a level of knowledge that would not be sufficient in classical teaching methods. This thesis deals with one such concept, the so-called Quantum Key Distribution (QKD).

Quantum Information Theory (QIT): Before QIT, the age of Information Theory had begun with the decryption of the Enigma by Alan Turing, one of the most influential people in early computer science. Later the starting point of modern cryptography can be dated to 1945, with the publication of the article "A mathematical theory of cryptography" by Claude E. Shannon [60]. Shannon proved that a perfectly secure encrypted message requires a just as long key. Today, technology is further along and has robust encryption methods that work well even with keys much shorter than the message itself [60]. For example, to test all combinations of a 128-bit key, one must try 10^{38} different combinations. Even if billions of computers in the world worked together, each capable of performing a billion calculations a second, it would take trillions of years to test all the combinations [72]. Despite the fact that the standard key length nowadays is 256 bits, there is still a crucial problem. Current encryption, like the RSA-Algorithm, is based on the so-called prime factorization or discrete logarithms. That means one has to do a prime factorization to crack the key, for which currently, computing power is not sufficient to do it in a reasonable time. In that case, polynomial-time complexity counts as reasonable. If the computing power improves, one can make the problem difficult (large) enough so that the faster computer is again not able to break it [54, 12].
However, suppose quantum computers replace the classical ones. The prime factorization and the discrete logarithm algorithms would be breakable in polynomial time using the *Shor* algorithm [59]. According to Google, this means that their quantum computer is 100 million times faster than a regular computer [75]. To be able to imagine this number and explain why a quantum computer is significantly better, Herman and Friedson have given an apt description: "a quantum system is able to look at every potential solution simultaneously and generate answers—not just the single 'best answer,' but nearly ten thousand close alternatives as well—in less than a second. This is roughly the equivalent of being able to read every book in the Library of Congress simultaneously in order to find the one that answers a specific question" [23]. These are only assumptions that will be clarified in the following decades, depending on the development of quantum computers. However, if the scenario occurs and quantum computers become ubiquitous, it could have fatal consequences since not only do private individuals depend on secure communication, but also banks, states, or even secret services need secure encryption. The day when a quantum computer can hack asymmetric encryption is called Q-Day. When this occurs, sensitive data is no longer secure, i.e., emails, credit card information, self-driving cars, military systems, or even our energy supply, to name a few examples [37].
Therefore humanity needs a new type of encryption that is no longer based on mathematics but can guarantee a security standard independent of computing power. In the best case, this type of encryption should also be implementable without quantum computer technology. To solve this problem, the physical laws of quantum mechanics come in handy.

2.4 Background QKD

Quantum Key Distribution (QKD) : Even though Shannon performed his proofs mathematically, in the practical conversion of these theories, the information must flow through a physical medium and therefore, is subject to physical laws. At the same time as the *information theory* originated, physicists have discovered the quantum mechanics and fundamentally changed the up to now existing worldview [8, 7]. If the transmission medium for information is provided now on an atomic level, one is subject to the laws of quantum mechanics. The combination of Information Theory and quantum mechanics is the Quantum Information Theory (QIT) [63].
Before going into the applications of QIT, a fundamentally important law of quantum mechanics needs clarification. A quantum object, for example, a photon, has a location and a velocity. This occurrence is since a quantum object is both a particle and a wave. The particle has a place but no velocity, and the wave has a velocity bot no place. However, a quantum object behaves either as a particle or a wave. Therefore, one can never simultaneously determine the place and velocity of such an object precisely. This is the Heisenberg uncertainty principle (HUP) [24]. Wiesner used this principle in the 1960s and created the first application of Quantum Information Theory. The idea was to make banknotes forgery-proof with the help of the HUP. Researchers encoded banknotes with identification information with the help of quantum objects. When an attacker tried to get all this information to copy the banknotes, it was, thanks to the HUP, inevitable that errors would occur, and part of the information would be lost or destroyed. Afterwards, the bank had to check the consistency of the banknotes information to see if it had been tampered with [64]. Since then, many other applications of QIT have been developed, including the quantum computer itself. Now to the application, which is a central topic of this bachelor thesis and has an answer to the requirements posed in chapter 2.3. In 1984 Bennett and Brassard developed the BB84 protocol, which also uses the laws of quantum mechanics to implement Quantum Key Distribution (QKD) [5]. The critical information (key) exchange between two parties (Alice and Bob) is inevitably safe with this protocol. By underlying physical laws, Alice and Bob can be sure whether the exchange has been eavesdropped or not. If the latter is the case, one must only repeat the protocol. Instead of classical bits (0 and 1), the two parties use qubits to share information. Such a qubit is typically a photon with a specific spin representing the binary numbers. Suppose now an eavesdropper tries to get this information. In that case, Eve has to measure the photon's spin and therefore runs the risk of falsifying the information and being discovered due to the HUP [5]. If now a key of the same length as the message is in usage, optimal encryption can be guaranteed, according to Shannon [60]. The thesis discusses detailed aspects of this protocol in chapter 4.2.
QKD is not based on mathematical scaling and works without a quantum computer [63], but still requires optical fibers, lasers, and optical measuring devices.
Further, we want to distinguish the terms of QKD from Quantum Cryptography. In the literature, one finds different terminologies, partly QKD and Quantum Cryptography are interchangeable. This thesis will use Quantum Cryptography as the generic term and QKD as a subdivision of it. QKD is a concept among others, currently still theoretical concepts, such as quantum encrypted message exchange. For the latter, even a quantum computer would be needed [63]. In cryptography and Quantum Cryptography, the key exchange is the initial step and plays a central role in encrypted information exchange. Even though, after the QKD currently, the encrypted communication still happens classically, it is nevertheless a good entry point into the field of Quantum Information Theory and probably, in some years, common knowledge for each computer science student [21]. For these reasons, the focus of this thesis will be on QKD only.

Title	Author	Reference
Analyzing the socioenactive dimensions of creative learning environments with preschool children	Carbajal et al.	[9]
Introducing a Paper-Based Programming Language for Computing Education in Classrooms	Mehrotra et al.	[47]
Exploring tabletops as an effective tool to foster creativity traits	Catala et al.	[10]
A multimodal approach to examining 'embodiment' in tangible learning environments	Price et al.	[51]
Designing tangible programming languages for classroom use	Horn et al.	[26]
Supporting Children's Collaborative Authoring: Practicing Written Literacy While Composing Oral Texts	Ananny	[1]
A tangible interface for organizing information using a grid	Jacob et al.	[28]
Topobo: a constructive assembly system with kinetic memory	Raffle et al.	[52]
Digital Manipulatives: New Toys to Think With	Resnick et al.	[53]
Tangible Interfaces for Structural Molecular Biology	Gillet et al.	[20]
An Active Tangible User Interface Framework for Teaching and Learning Artificial Intelligence	Raffaele et al.	[15]
Explaining multi-threaded task scheduling using tangible user interfaces in higher educational contexts	Raffaele et al.	[14]
Enabling the Effective Teaching and Learning of Advanced Robotics in Higher Education using an Active TUI Framework	Raffaele et al.	[13]
Sifteo cubes	Merill et al.	[48]
A Tangible-Tool-Based Lesson Plan on Cipher Key Exchange Protocol for Early-Stage Learners	Khan et al.	[36]
The BBC micro:bit: from the U.K. to the world	Austin et al.	[3]

Table 3.1: A list of all TUIs, which we considered for our Design Space

3 Related Work - a TUI Design Space

This section refers to related work on Tangible User Interfaces (TUI), from which most intend to transfer knowledge. An extensive literature review on the subject of TUIs forms the basis for this chapter. We were able to select 18 TUIs from 16 papers for this purpose. We present a design space that considers the design, look and functionalities of different TUIs. Regarding the topic of the thesis, a particular focus lies on learning with the technology. Although two of the eighteen selected TUIs have no application in the educational area, they are still valuable to the design space and, therefore, also relevant. With every subsection, one can see a MindMap, visualizing the subsections topics. In the table 3.1 one can see the sixteen selected papers.

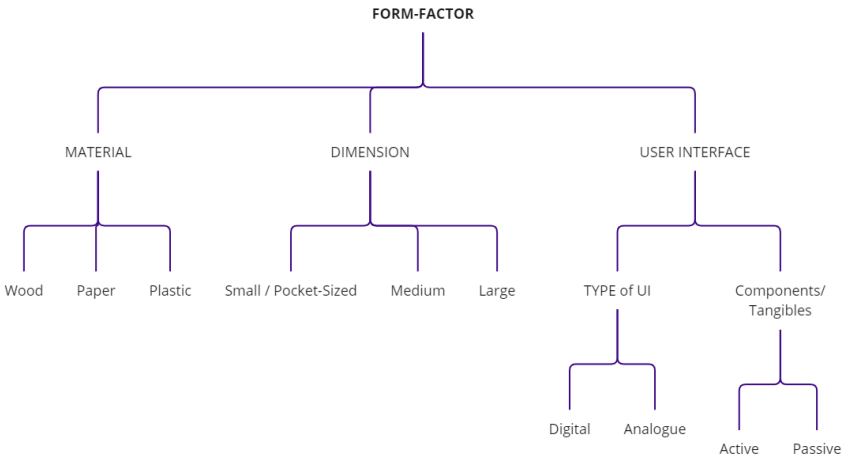


Figure 3.1: Visual Mind-Map Chapter Form Factor

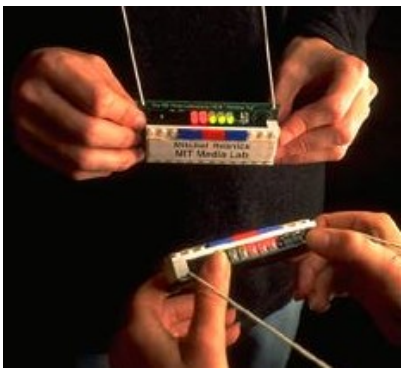
3.1 Form Factor

As mentioned before (see chapter 2.2), TUIs have diverse forms and characteristics. By comparing the eighteen TUIs, we could break down three categories, which decisively determine the form factor. The dimension of the TUI, the material used, and the User-Interface (UI) (see figure 3.1).

3.1.1 Dimension

The eighteen TUIs are deliberately not divided into categories of absolute numbers, as this is not applicable outside the papers under consideration. Nevertheless, distinguishing TUIs concerning their size also works by relative descriptions of each other.

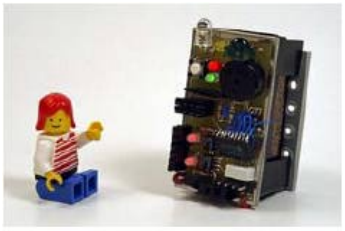
Small-TUIs TUIs that can be held or operated with one hand appear to be the smallest. They are part of the *small* category. Pocket-Size format is also an appropriate term. An optimal example are the Sifteo Cubes (represented in the figure 3.2b). These are rectangles the size of a hand with an integrated touch display. The unique thing about them, one cube is as functional as if they are plugged together. The value of this function depends on the application and the user. The cubes receive the information through a wireless connection to a computer, which they then can display. Merill et al. used the cubes to make the concept of object-oriented programming (OOP) easier to understand. Therefore the cubes shall represent the interaction and dependencies of objects in OOP using C-*sharp* as an example [48]. Another small TUI are Thinking-Tags (represented in the figure 3.2a). These tags are worn around the neck and fit in a hand or a pocket. When two people with these tags meet, the tags exchange information. A light turns on when both people have common interests. The user stored these interests previously in the tags database. This technique has been used at conferences to reduce the hurdle of a first conversation and make it more comfortable to meet new people. One can also use Thinking-Tags for educational purposes. Pre-college students used the tags to simulate the concept of viral spread. There were “infected”-tags, “immune”-tags, and “healthy”-tags. The students could simulate a pandemic and visualize how the virus spreads from person to person by evaluating the tags’ meta-information afterward. The students developed new theories and, therefore, tested new settings [53]. More examples examples for small TUIs are Beads for creating dynamic patterns of light and Crickets for creating communities of interacting robots to learn about principles of communication [53] (see figure 3.2).



(a) Thinking-Tags TUI [53]

(b) Sifteo Cubes TUI [48]

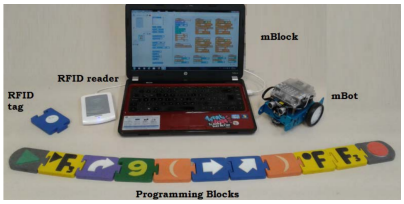
(c) Beads TUI [53]



(d) Crickets TUI [53]

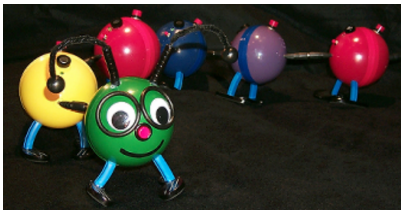
Figure 3.2: Pictures of Small-TUIs

Medium-TUIs Medium-sized TUIs no longer fit easily into a pocket. They are held and also operated with two hands. Nevertheless, one can look at the TUI entirely at a glance. TellTale, e.g., is a TUI that strongly resembles a giant caterpillar. This caterpillar consists of five body parts and a head. Each part has a record button and is used to record twenty seconds of voice or sounds. Next to the record button is a play button, which can play back the recorded voice. The idea is to give preschoolers a TUI to practice telling a coherent story divided into individual parts, represented by the caterpillar body [1].
Python-Molecular-Viewer-TUI (PMV-TUI) is a 3D model TUI of molecular particles. These are held with both hands in front of a camera and viewed through a display. Through Augmented-Reality (AR), the molecular particles can be manipulated and observed. "Users can easily change the overlaid information, switching between different representations of the molecule, displays of molecular properties, or dynamic information [20]." The goal was to determine if the TUI with AR had real advantages over a simulation or visualization [20]. The section 3.5 describes these advantages. More examples of medium TUIs are TaPrEC + mBot [9] and TERN [26], both are tangible programming environments for children (see figure 3.3).

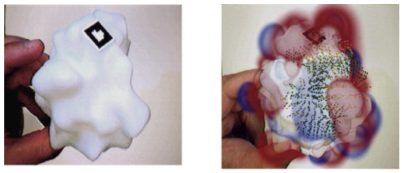


(a) TaPrEC + mBot TUI [9]

(b) TERN TUI [26]



(c) TellTale TUI [1]



(d) PMV-TUI [20]

Figure 3.3: Pictures of Medium-TUIs

PaPl [47]	Rube-Goldberg TUI [10]
“Diffie-Hellman-Key-Exchange TUI” [36]	Senseboard [28]
“Table Top Horse Race” [15]	“Table Top Multi Threading” [14]
“TUI Robot Operating System” [13]	LightTable [51]

Table 3.2: Large Sized TUI List - All large TUIs from our Design Space

Large-TUIs To put it simply, large TUIs are everything above and beyond. Most of the TUIs in our research belong into this category. Especially TableTop TUIs are often designed so that several people can work together and operate at the TUI simultaneously. In the Large-TUIs list 3.2, one can find all TUIs from this category. The Rube-Goldberg TUI is a tabletop, which, as the name suggests, is supposed to simulate a Rube-Goldberg machine (This is one of the two TUIs without an educational context). The goal is to get a ball into a target by building a path. On display, the ball was simulated, as also the blocks and connectors for the path. Latter is built or manipulated through tangible pucks. Therefore users could interact with the TUI and, e.g., place blocks or copy and delete them. Once the user had finished building and started the simulation, the ball began to roll. This TUI is large enough to allow more than one person to work on it to build a path together and achieve the goal [10]. The second example, also a non-educational TUI, is Senseboard. Senseboard is a whiteboard with a grid. The tangibles, in this case, small pucks, are placed in the cells specified by the grid. These pucks contain information that can be used for scheduling work or organizing tasks. The significant advantage over a regular whiteboard is expanded functions, which lead to displaying additional information. With the help of the pucks, a user can call these functions by placing them in a grid cell. Thus a reduced, clear view can be generated consciously. The user can extend this view if necessary [28].

3.1.2 Material

As far as the choice of materials is concerned, there are no limits for the TUI designer. It does not always have to be the highest quality or most expensive material to create a decent user experience. According to the application, the material used should correspond. Whether this is significant is unknown [41]. The materials of the CPUs and technology used in the TUIs are deliberately left out. We focused on the materials the user comes into contact with.

Plastic The most common material we found is plastic. However, there are differences here as well. LightTable, a TableTop TUI with which concepts of light are to be made visible, deliberately plays with different densities, thicknesses, and colors. The TUI emits a white-glowing light beam on acrylic glass. Twenty children (ten to eleven years old), each in pairs, could then place different objects into the emitted light. Due to the different tangibles, the light reacts accordingly. This TUI offers a playful way for children to engage with concepts of light, such as refraction. They get a feeling of how the light behaves without knowing the correct term, which would be too complex for this age [51].

Wood A more sustainable alternative to plastic is wood, as in the case of TERN, a programming TUI. Users can plug single wooden blocks into each other to create a program sequence. This program sequence can be a robot movement, for example. The children can see symbols on the blocks representing the according function (e.g., turn, move forward). The goal is to introduce children to programming without dealing with a graphical user interface, which would probably be too demanding or challenging for this age. Further, wood makes the programming blocks look like ordinary building blocks that children are already familiar with. The significant advantage of TERN is that no syntax errors can occur since the blocks only fit together if a syntax error is impossible. Latter is possible through unique connecting pieces [26].

Paper The last material that this thesis illuminates is paper. Even though only two TUIs from our list uses this material, it is worth mentioning to show that it is possible to build a budget-friendly and well-functioning TUI. Because of the budget-friendliness, it is reproducible and, therefore, also possible to sell in larger quantities to schools. One of the TUIs in question is called PaPl, a paper programming language. Instead of blocks, as in TERN, paper snippets are used. These are placed in predefined lines, resulting in a program. An accompanying camera or a laptop's webcam reads the lines of code. The laptop or computer connected to the camera interprets the lines of paper-code and executes the program. One can easily install this kind of TUI in any classroom with at least one computer (plus camera) or laptop. The target group here is ten to nineteen years old. The challenges can be customized accordingly. As with TERN, this TUI gives students a more comfortable and intuitive introduction to programming [47].

Of course, these materials are only a fraction of what is possible for a TUI. Li et al. emphasize that the material choice is essential because it can influence the user experience and possibly even the learning success with the TUI [41].

3.1.3 User Interface

There are many different ways in which a user interacts with a TUI. This interaction does not have to be necessarily digital. For example, pushing a TellTale record button is more of an analog than digital interaction. Apart from the technology built into TellTale, the interaction between the user and the system is purely physical and does not involve digital displays [1]. From the sixteen papers, we considered, one can also see that screens are usually not present with a target group under fifteen. Latter suggests that interaction with a display may not be suitable for a younger target group as the complexity associated with a display increases. The Rube-Goldberg TUI, for example, has a digital user interface. The primary interaction takes place on display [10]. (Other examples for the digital UI are the Sifteo Cubes [48] or the TableTop Multi-threading TUI [14]). TUIs' accompanying components/input devices are typically tangible, as in the Rube-Goldberg TUI [10]. The tangibles can play an active or passive role. In some TUI, the user must actively use tangibles to perform an action or manipulate something. An example of this is Senseboard. Without the active participation of the pucks, the function of the extended information would not be usable. Thus, the advantage over classical work organization would be lost [28]. The tangible has a passive role in the PMV-TUI. Here it is only used to have something touchable, but the tangible itself cannot influence anything in the 3D molecules since this is only related to the AR functionality [20].

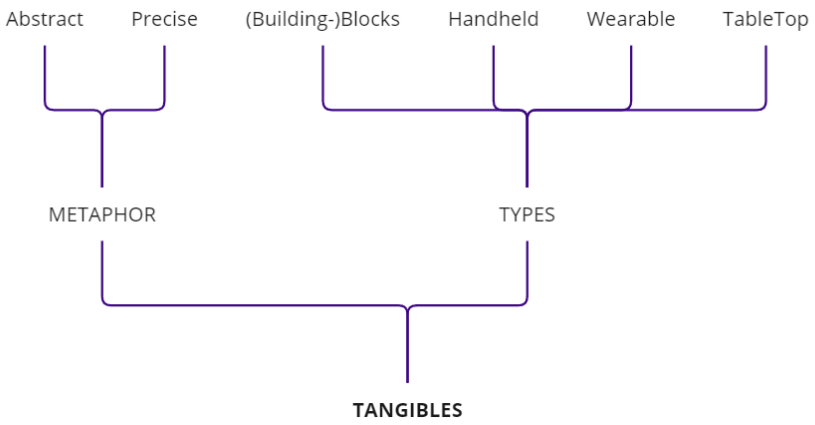


Figure 3.4: Visual Mind-Map Chapter Tangibles

3.2 Tangibles

This paper mentioned the term tangibles several times now. Besides being part of the name, tangibles are an essential concept for TUIs. Tangible objects are a unique selling point and differentiate TUIs from other HCI technology. This section will explain which forms tangibles can take and how to use them (see figure 3.4).

Types As with the materials, there is no concrete limit to the forms and types of TUIs that can appear. Nevertheless, one can recognize patterns, and which types of tangibles occur in other research papers. We have extracted four fundamentally different types from the sixteen papers. Again, these are not all of them and could be defined differently. The four types are *handheld-, wearable-, TableTop-, and building-block tangibles*. Except for the TableTop tangibles, all the others have defining names.
Nevertheless, a brief explanation is in order. A handheld-tangible is, for example, the 3D printed PMV-Molecular [20]. The user holds it with both hands, but there is no additional function besides twisting or turning it upside down. The Thinking-Tags are wearable tangibles [53]. One can annotate that they are also handheld, but the fact of being wearable outweighs the handheld fact. It is similar to a square being also a rectangle. TERN and TaPrEC are both examples of building-block tangibles [26, 9]. The developer chose this analogy deliberately concerning the targeted group, which is children who already know how to use building blocks and, therefore, can operate the TUIs very naturally. However, TableTop tangibles requires some more explanation. The shapes of the individual TableTop Tangibles can differ significantly, but the purpose they serve is the same. A TableTop tangible manipulates what is shown on the TableTop to achieve a particular goal. Usually, (RFID) tags help a camera inside (or outside) the TUI recognize the tangibles and assign them to a specific function. The output result depends on the location on the TableTop and the function the tangible is supposed to perform.

Mataphor The represented analogy from a tangible is the so-called metaphor. Tangibles represent a particular function and serve to illustrate certain concepts. The visualization of a function can be deliberately abstract or precise. One can find an exact representation in the Multi-Threading-TUI. Here the tangibles represent the individual processes that the user has to schedule. Each tangible has a symbol on a wood block, reflecting what process it is. For example, a zipped folder represents file compression. In an abstract representation, the TUI Designer can deliberately choose to simplify complex structures, and concepts [14]. In contrast, the TUI Table Top Horse Race is not about a horse race but about Artificial Neural Network (ANN) concepts to be conveyed. The tangibles look like objects from a horse race but represent something regarding an ANN. The horse illustrates the context simulator controller, clouds the hidden layer nodes, a finish podium, the output visualization, and a Speedometer, the input speed value. These are not all tangibles used for this TUI, but the idea remains the same: A “horse-racing analysis contextual example was adopted to explain the artificial intelligence algorithm. This context simulated the relational model of horse race time based on parametrical data of speed and health” [15].

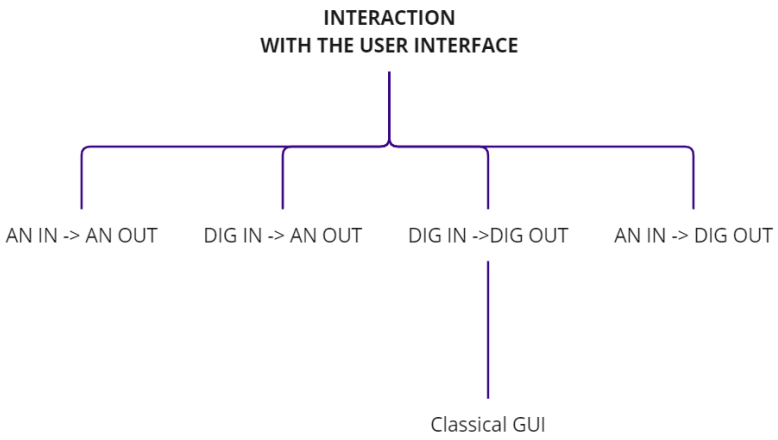


Figure 3.5: Visual Mind-Map Chapter Interaction with the User Interface

3.3 Interaction with the User Interface

Not only does the TUI itself consist of digital and analog components. The interaction with the user interface also fits into these two categories. Since a TUI is an HCI technology, there is an interface between human and machine, as with all others. The human interacts with the TUI, and the input is processed, resulting in an output. Four types of interaction can now be derived (see figure 3.5).

1. analogue input -> processing -> analogue output
2. digital input -> processing -> analogue output
3. digital input -> processing -> digital output
4. analogue input -> processing -> digital output

3.3.1 Analogue Input -> Analogue Output

At first sight, analog input resulting in analog output seems illogical regarding TUI technology. With the TUI Topobo, however, this is the case. With building blocks, one can assemble an animal or a creature and bring it to life. There are static (passive) and motorized (active) building blocks. Cables connect the latter. If the user now presses a record button, they can record a movement with the active parts by turning, pressing, and pulling. The movement is played back after the recording [52]. The user interface here is the built creature itself. This interaction is an analog for in- and output since nowhere is a display or comparable digital components involved. Another example is TaPrEC & mBot. Here, as with TERN, children plug single programming blocks together to write a program. These are then read in with a reader tool, processed by an external computer, and sent to a robot that executes the commands. Again, physical input from the human and physical output from the robot [9].

3.3.2 Digital Input -> Analogue Output

BBC: Micro Bit is a TUI that gets a digital input and results in an analog output. It is a single-board computer, a similar, more simplified version of an Arduino or Raspberry Pi. With the reduced complexity, a younger target group should have their first experience with programming. The digital input works via an interface on the computer. This interface supports the user to program the Micro Bit. The output results in LEDs attached to the TUI, giving feedback or representing individual letters or numbers. It is far from being an actual display and, therefore, an analog output [3].

3.3.3 Digital Input -> Digital Output

We did not find a TUI that suits this category, but there might be one. Instead of giving an example, this subsection shall define the requirements for a TUI fitting in this category. The problem is the lack of physical interaction between the user and the TUI. If both the input and the output are digital and run via a graphical user interface, the user would not have to touch the TUI or its tangibles to operate it. So can it be a TUI without a tangible? This example is more like a classical computer than a TUI. However, classical GUIs are often part of a TUI, used as a responsive part or for information display, as one can see in the next subsection.

3.3.4 Analogue Input -> Digital Output

This interaction often comes with TableTop setups and is the most common in the considered papers. The user commonly takes a tangible object and puts it on the display, which reacts to the tangible. An example of this is the Multi-Threading TableTop. There are CPUs and threads pictured on display, ready to get some tasks. Students have to assign processes to each CPU/thread in this setup. Tangible objects represent the processes. One tangible at a time is to objectify a process. The user can now place them on the TableTop display in the appropriate positions. As soon as the TUI has recognized the tangible, it visualizes the corresponding sub-tasks for the process graphically. In addition, the CPU utilization and total execution time are adjusted accordingly on the GUI [14]. There are also non-TableTop TUIs for this category. For example, PaPl, the paper-based programming language. Here a command sequence can be set with the help of simple paper programming blocks. A camera then captures the latter and translates it by the connected computer [47]. This simplified form of programming provides students (18-19y) a more straightforward introduction to programming, although their knowledge would not yet be sufficient for classical code.

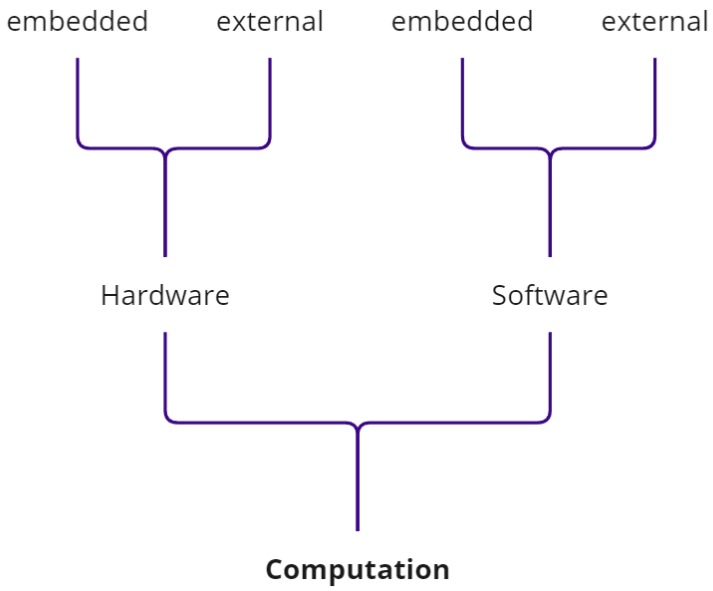


Figure 3.6: Visual Mind-Map Chapter Computation

3.4 Computation

As with other HCI technologies, the TUIs functionality depends on hard- and software. According to the purpose and other dependencies such as form factor, hardware and software can be part of the TUI (embedded) or only play to the TUI (external). This section only concerns computational hardware with a power supply to be able to execute corresponding computations (see figure 3.6).

3.4.1 Software

External In the TableTop Horse Race TUI (represented in figure 3.7), the creators implemented a bi-directional communication between a server and a client. The hardware of these tangibles consists of an Arduino NanoTm, a small LiPo battery, and a Bluetooth communication module. This communication module allows data exchange between servers and clients (tangibles). Even if the tangibles perform simple calculations, the entire logic, and thus the software, is on the server, which is independent of the TUI. So the software is not integrated into the TUI, and therefore external [15].

Embedded In contrast, the developers tightly integrated the software within the Sifteo Cubes. The embedded software allows the cubes to work individually and communicate if the cubes are plugged together by the user [48]. The argumentation to divide hardware into external and embedded work analog.

Figure 3.7: TableTop Horse Race TUI [15]

3.4.2 Hardware

External PMV-TUI is an example of external hardware. From the description of the TUI, it is clear that AR-enhanced molecules the user views through a display. Latter is attached to a classical computer. The 3D molecule has neither a power supply nor any integrated computational hardware. One can argue that the computer is part of the overall concept and thus part of the TUI, but the computing power is not part of the object the user interacts with, and thus external [20].

Embedded A TUI with integrated hardware is Beads. The user can wear it as a necklace or bracelet. With the help of beads, children can explore the behavior of decentralized systems. By being able to program the beads, children also "learn about programming paradigms." For this purpose, all programmable beads have a built-in microprocessor and LED. The individual beads communicate and influence each other." [53].
Even if the transitions from external- and embedded hardware are fluid, one can take it as a clue to which part the power supply is connected. This part is usually provides the computational power.

Title	Author	Reference
Introducing a Paper-Based Programming Language for Computing Education in Classrooms	Mehrotra et al.	[47]
Exploring tabletops as an effective tool to foster creativity traits	Catala et al.	[10]
Topobo: a constructive assembly system with kinetic memory	Raffle et al.	[52]
Digital Manipulatives: New Toys to Think With	Resnick et al.	[53]
Tangible Interfaces for Structural Molecular Biology	Gillet et al.	[20]
An Active Tangible User Interface Framework for Teaching and Learning Artificial Intelligence	Raffaele et al.	[15]
Explaining multi-threaded task scheduling using tangible user interfaces in higher educational contexts	Raffaele et al.	[14]
Enabling the Effective Teaching and Learning of Advanced Robotics in Higher Education using an Active TUI Framework	Raffaele et al.	[13]
Sifteo cubes	Merill et al.	[48]
A Tangible-Tool-Based Lesson Plan on Cipher Key Exchange Protocol for Early-Stage Learners	Khan et al.	[36]
A Meta-Analysis of Tangible Learning Studies from the TEI Conference	Li et al.	[41]

Table 3.3: A list of all papers, which we considered relevant regarding the impact TUIs have on the learner

3.5 Learning with TUIs

Two central questions are clarified. First, in which environments TUIs are used for learning, and second, what effects do TUIs have on the learner. Sixteen of the eighteen considered TUIs serve the educational domain. 50% of the TUIs had the purpose of teaching computer science concepts. The other topics considered are physics, biology, communication, and robotics. The studies represented almost every age between four and 24+ years. A classification into age categories is not conducive at this point due to overlaps of the age groups. The results of eleven studies with TUIs from the field of education are relevant regarding the impact TUIs have on the learner (represented in the table 3.3). However, all eleven studies provided neutral to positive results, probably related to the fact that negative results are less likely to be published (see figure 3.8).

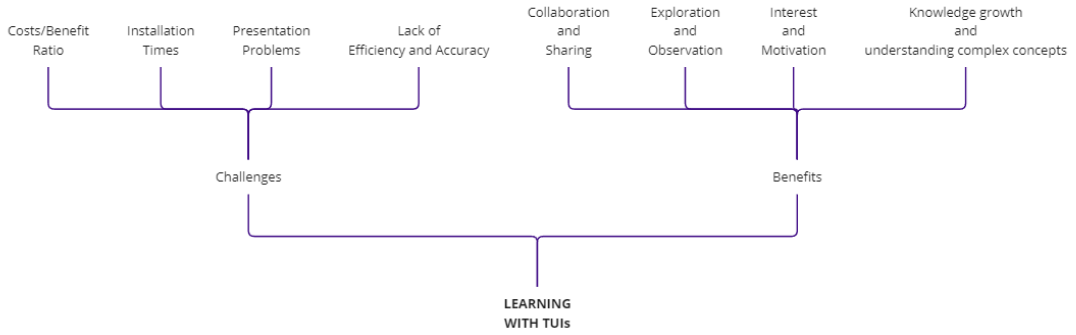


Figure 3.8: Visual Mind-Map Chapter Learning with TUIs

3.5.1 Challenges

The opposing side on learning with TUIs is covered in the meta-analysis "Tangible Learning Studies from the TEI Conference" by Li et al. [41]. Even if the arguments are partly somewhat more general than only the learning aspect, they are still valuable and applicable for TUIs serving the educational context. The meta-analysis calls these arguments challenges. Li et al. collected challenges from four perspectives. First, users had concerns about costs and installation times. Second, they found it difficult to represent complex situations and achieve a certain level of abstraction. Third, the developers had concerns about the cost/benefit ratio and technical reliability. Fourth, they felt that the efficiency and accuracy of a learning activity could suffer from a TUI. In addition, deviation from sense and purpose could cause disinterest. Besides the other groups the teachers' concerns, were the most relevant regarding this section and the challenges of learning with TUIs. As a final argument, they said that the "Drive to make "cool" tech, ignore the abstraction; and shoehorning technology into space/situation where that technology is not helpful or needed" [41].

3.5.2 Benefits

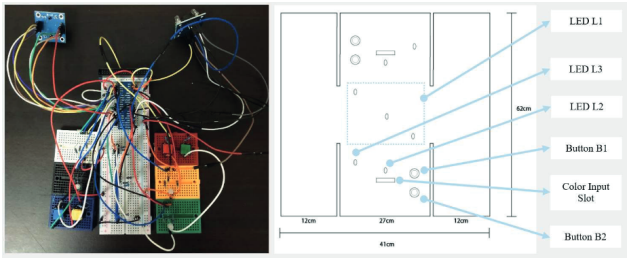
In contrast to the challenges, the positive effects on the learner are not only more concrete but also clearly outweigh the challenges.

Collaboration and Sharing The characteristics of an interactive user interface in combination with tangible objects are particularly suitable for sharing them within a group [10]. People can benefit from group work. In the study with PMV-TUI, the researcher found that the TUI led to a collaborative discussion about the topic, despite being operated by only one person. The same effect Mehrorta et al. stated with PaPl [47, 20]. In addition, TUIs supporting working in groups can motivate the formation and testing of new theories. The latter was the case, for example, when MIT students used Thinking Tags to simulate a virus wave. The evaluations afterward allowed them to form new theories and test them in a different setting [53].

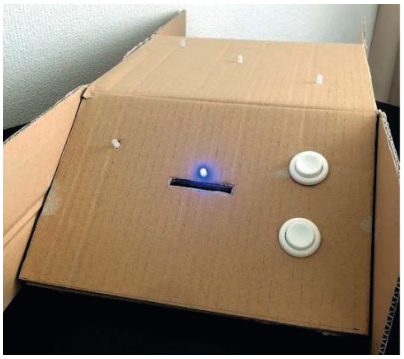
Exploration and Observation To get a holistic overview, the user can move either the TUI or himself around it, depending on the TUIs size. For more detail, the user only has to adjust the angle of view to the TUI and possibly move closer to the object. TUIs, therefore, offer a holistic and detailed overview at the same time as "Extending observation and contemplation" [20]. The natural mechanisms to manipulate a TUI support the explorative approach [20]. The latter results in an intuitive way to operate the TUI, support explanations and conceptualization. With an apt TUI design, people can use it without a manual.

Interest and Motivation For the TUI Robot Operating System, Raffaele et al. did a study to find out if the TUI is better than a traditional lecture regarding learning success. They found that the students from the TUI test group were less distracted by their own devices than in the traditional lesson. They also showed more interest in actively participating in the lesson [13]. Merrill et al. from Sifteo Cubes also showed a higher interest in the TUI presentation, which led to higher motivation in the learning process [48]. The motivation is possibly also induced by a stronger flow of thoughts, as described in the example of RGB [10]. Interestingly, the researchers found a higher motivation in the corresponding test subjects when trying to teach C-*sharp* OOP using the Sifteo Cubes; the professor's motivation and thus his teaching activity increased. Merrill even goes as far as to claim that the teaching activity was of higher quality [48]. Further, the MIT group's test with the Thinking Tags went clearly beyond the classical motivation. They described the whole study as a richer learning experience, which would not have been possible with traditional computer support or group work [53].

Knowledge Growth and Understanding Complex Concepts TUIs can positively influence learning. Nevertheless, the central question remains whether this applies to newly acquired knowledge. Furthermore, it is interesting to see how TUI learning relates to classical lectures and/or GUIs. Three studies addressed these two questions. All three studies were structured similarly, each with a different TUI and topic. They all involved participants from the higher education/university sector (students). The three objectives of the studies were "teaching and learning ANN concepts,"[15] "understanding multi-threaded task scheduling"[14] and programming by undergraduate IT students, and "explaining Robot Operating System (ROS)" [13] based sensor network topologies. After a pre-lecture and test, the researchers divided the students into quasi-equal groups. One of which was allowed to use the TUI to learn the given topic. In contrast, the other group had to attend a classical lecture or learn with a GUI. Afterwards they conducted a post-test.
The TUI groups performed significantly better post-test results in all three studies, provided that the pretest results were comparable. With the ANN concepts, a knowledge gain of 32% more was determined than with the GUI variant. The Multithreading TUI scored a 22.8 higher mark and with ROS 42,9% knowledge was gained (Lecture knowledge gain: 28,3%) [15, 13, 14].
In the chapter 2, we mentioned that through computer-based education concepts, students could understand concepts that are too complex for the current level of knowledge. This advantage works particularly with TUIs. Through the help of Topobo, seven to thirteen-year-old children learned about "Balance, Center of Mass/Center of Gravity, Coordination, Relative motion, Movement with Multiple Degrees of Freedom, Relationships between Local and Global Interactions [52]." Raffle et al. suggest that Topobo can help teach principles of physics, kinematic systems, modular robotics, and system coordination that are otherwise subjects at the earliest in high school or college [52]. Raffaele et al. of ROS speak of the potential of TUI architectures to mitigate the challenges of teaching and learning abstract and complex concepts in higher education [13]. Encountering heavy concepts always brings a set of obstacles that users can overcome with an educational technology like TUIs [15]. Besides the students also, the teachers benefit from TUIs. The TUI not only provides a more accessible understanding of a topic but, conversely, it also provides a platform to explain topics that are difficult to explain without the help of educational technology [14].



(a) Inside the DHKP-TUI [36]



(b) Outside of the DHKP-Box [36]

Figure 3.9: Diffie-Hellman-Key-Exchange-Protocol (DHKP) -TUI [36]

3.5.3 TUI for Understanding Cryptography

One paper, in particular, should be highlighted as a conclusion to this chapter. Kahn et al. have built a TUI to help early-stage learners understand the Diffie-Hellman key exchange protocol (DHKEP). This paper is unique because it is the closest to this bachelor thesis regarding content and motivation. Inspired by the computer science unplugged concept, they built a display-free TUI. Since TUIs improve learning, Kahn et al. benefit from them by making complex concepts understandable to early-stage learners through TUIs. The TUI they have built is designed simple but ingeniously. To properly use the TUI, it takes two people, representing Alice and Bob. To explain the DHKEP, they make use of a common color analogy. Here, instead of calculating with powers and the modulo operation, they use color to show how from publicly known information, a private key can be generated (color mixed). In the TUI, LEDs connect to a Raspberry Pi and represent the colors and their mixtures. A cardboard box hides the Raspberry Pi and is the basis for the LEDs and the buttons for Alice and Bob. The creators deliberately designed this box so Alice and Bob could only see their private information. All other publicly exchanged information is visible on a shared “bridge” (see figure 3.9b). A user study showed increased engagement, collaboration, and comprehensibility. Furthermore, they asked the participants (higher education students) which age group they would recommend the TUI. The age group twelve to fourteen received the most votes, which again indicates that a TUI can significantly reduce the level of complexity. In addition, the researchers emphasize that they have built a very cost-efficient and eco-friendly version that can help reduce the level of complicity and “spread quality education in developing nations and contribute to the universal access to education movement [36]” (see figure 3.9).

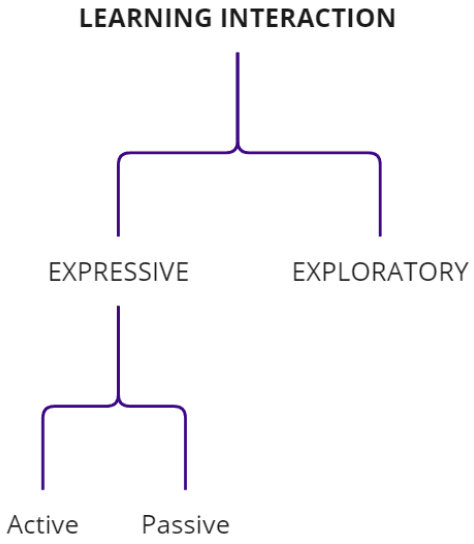


Figure 3.10: Visual Mind-Map Chapter Learning Interaction

3.6 Learning Interaction

Learning Interaction is a discipline that exists independent of TUIs. That is why this topics section is separated from chapter 3.5. In order to internalize concepts, especially with TUIs, there are two different ways to proceed. One is the e*xplorative*- and the other is the *expressive*-way. Which one to use is a design decision and not in the hands of the end-user. In the paper from Paul Marshall, this discipline is a sub-item of a framework that can be taken care of when developing a TUI for learning [44] (see figure 3.10).

Exploratory Interaction In the exploratory process, the user tries to discover and understand the underlying concepts or representational model of the TUI. The topic and its representation are predefined by an expert and given to the learner to discover. The newly discovered concepts can be related to the user's experiences or prior knowledge about the topic to gain new insights [44]. The TUI LightTable is an apt example. This TUI supports explorative learning very well. The theoretical model of light can be discovered playfully through the different tangibles, such as lenses, mirrors, and more, as the children place the objects in the light beam and thus learn in an explorative way how light behaves [51]. The goal of the exploratory-way: The less cognitive effort is required to operate a system, the more focus a user can place on the underlying concepts [44].

Expressive Interaction In the expressive activity, the user must take action and create something to express his idea about a given topic or domain. TUIs can support users in expressing or implementing these ideas concretely. After creating their representation of the given topic, users can reflect on it and therefore learn something from their own creation [44]. An example to better understand this kind of learning is Topobo. It is the same example Paul Marshall uses in his paper. Here the tangibles used to build the figures are the aids to the self-created representation. The specially created movement for each creature can be analyzed and adapted if necessary [52].

4 QKD-TUI Requirements

4.1 Suitable Scenario for the QKD-TUI

In order to build a proper Tangible User Interface (TUI), not only the TUI itself must be considered. The place of use, or the scenario, plays a decisive role in design decisions for the TUI. The research so far has been very one-sided in terms of scenarios. The education domain is the most common scenario in the literature (see chapter 3). Specifically, fourteen of the eighteen described TUIs one could subordinate in the education domain. Almost none of the papers considered providing their TUI (concept) in a different scenario. This paper, however, deals with where an explanation for Quantum Key Distribution (QKD) is needed and for which group of people.
The results of a questionnaire-based online user study conducted by Delgado Rodriguez et al. served as a basis for answering these questions. In this survey, experts from the field of QKD answered in which scenarios they already had to explain QKD and which explanation tools they used. In addition, they assigned corresponding target groups to the individual scenarios. The attendees assessed their expertise and motivation on the QKD subject for the respective listeners. In addition, the survey also considered hypothetical scenarios. Like the real ones, the scenarios were each associated with the persons and the tools. The experts who had not yet experienced the corresponding real scenario answered for the hypothetical scenarios. The following six possible scenarios were considered:

1. “A marketing scenario where you explained something about QKD to someone to sell a product or idea.”
2. “An external presentation scenario, where you explained something about QKD to someone in order to present your company/project externally (e.g., to external visitors or trade fairs).”
3. “An internal presentation scenario where you have explained something about QKD to someone who is part of their company or project.”
4. “An exhibition scenario, where you have explained something about QKD to someone as part of an exhibition (e.g., in a museum).”
5. “A teaching scenario, where you have explained something about QKD to someone as part of a teaching lesson/lecture/seminar.”
6. “A private scenario where you explained something about QKD to acquaintances, friends, or relatives (e.g., to tell them about their job).”

The possible tools for an explanation were *video, audio, text, experiments, simulations, pictures, slides, none,* and *other*.
First, it is clear from the study participants’ responses that QKD is difficult to understand and not easy to explain. Further, when participants attempted explanations, they were only partially understandable. We cannot test the explanation’s nature because they are unavailable. However, it is possible to check which tools the experts used for their explanations. Across all scenarios, the preferred tools were *pictures, slides, text,* or *none*. Since the explanations were insufficient, the tools did not contribute enough to make the topic understandable. So there is potential for improvement and the need for other explanation material to increase its quality and improve understanding. The idea is to use a TUI at this point. Now the question arises, in which scenario a TUI is useful. It is essential to clarify this question because the scenario selection also influences the design decisions for the TUI prototype.

Scenario	Simulation	Experiment	Other	Total SUM
External	7	5	1	13
Internal	5	5	2	12
Exhibition	5	6	1	12
Teaching	5	5	2	12

Table 4.1: Final Results for the Scenario Selection

Indeed, a TUI is not suitable for every situation and every target group. Without statistical methods, the first scenario we rule out is the private scenario. Regardless of the ultimate size or transportability of the TUI, it is not very likely to always carry a TUI designed for a private scenario when the need for an explanation for QKD (coincidentally) exists. So that leaves the *marketing, external, internal, exhibition, and teaching* scenarios. TUIs have two decisive advantages. On the one hand, as one can see in the section 3.5, they are motivational. On the other hand, they reduce the entry barrier into a complicated topic by decreasing the complexity.
There are several target groups per scenario, e.g., in a teaching scenario, there are the target groups *pupils, students,* or *colleagues*. For each target group of each scenario (real and hypothetical), the study participants indicated, using a five-point scale (0-4), how they assess the expertise and motivation of the target group regarding the topic. In order to benefit from the described TUI advantages, only specific scenarios are suitable. Scenarios including target groups with an expertise less than or equal to two and a motivation greater than or equal to two on the five-point scale are suitable. With the expertise of three or more, there is no advantage to having a tool that facilitates barriers to entry if they do not exist in the first place. With a motivation of less than two, the motivational ability of a TUI from a scientific standpoint is insufficient to have enthusiasm for a topic at a level where the resulting learning effect is present. Every scenario except *marketing* had at least one target group that met these requirements. So what remained were *external, internal, exhibition, and teaching scenario*.
In addition to the target group assessment and the tools used so far, the participants selected which tools they would like to see in which scenarios. The choices were the same as those already used. Despite the insufficient explanations of current tools, the same tools again got many votes. For example, in the median, the favored desired tool in hypothetical and real scenarios was still the *pictures*. Similarly, slides were in a split-second place in the actual experienced scenarios. Nevertheless, the statement from the beginning that these tools were lacking holds. Therefore, the already most used tools are left out, while focusing on TUI-compliant tools. In addition, we exclude *audio* because it performed the worst in the median of all total desired tools (real and hypothetical). The tools considered for the final scenario selection are *simulation*, *experiment*, and "*other*." Simulations can be implemented well in TUIs. Examples of this one can find in the chapter 3. The category "*other*." describes new, still unused techniques. TUIs fulfill this category. We excluded *video* because it is not a typical medium for a TUI, at least not from the papers considered.

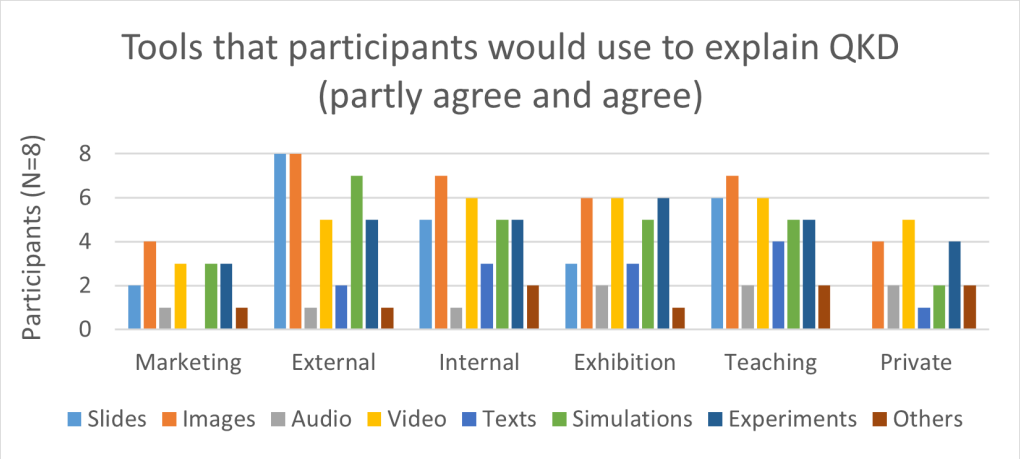


Figure 4.1: A plot from the survey by Delgado Rodriguez et al.

Now the three tools must be combined with the four remaining scenarios to select a suitable scenario for a TUI. In the survey there was a plot which combined all the votes (partly agree and agree) from the QKD experts for using a tool per scenario (see figure 4.1). Next, we only considered our three selected tools (*simulation*, *experiment*, and "*other*") and counted the votes (see table 4.1). The *external presentation scenario* was selected based on the most votes (13 Votes). *Internal, exhibition and teaching* each received a total of 12 votes from the QKD experts. The selection of *external presentation scenario* now also impacts design decisions for the TUI. In an *external presentation scenario*, the goal is to present QKD to, for example, a project or a company. In our case, the TUI should raise awareness and interest and explain QKD using the BB84 protocol. Such an *external presentation scenario* is possible, for example, at trade fairs or also at (external) visits. One should note that in this scenario, it is impossible to foresee who will eventually use this TUI and especially what level of knowledge this person has. The following implications arise:

1. It must be assumed that in an external scenario, the ultimate users of the TUI will have heard something about QKD or the BB84 protocol. The latter means that even without prior knowledge, the user must understand the concept of QKD through the BB84 protocol.

2. The TUI must therefore convey the protocol's purpose without going into too much detail about the physics behind it.

3. Representations of protocol aspects, such as filters or the photons, must be abstracted to an appropriate level.

Now it must be clarified which aspects of the BB84 protocol are essential for the basic understanding.

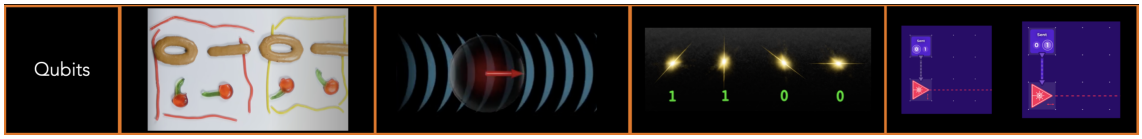


Figure 4.2: BB84-Aspects: Qubits visual examples

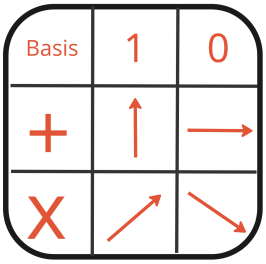


Figure 4.3: An example matrix for assigning bases and bits to polarizations

4.2 BB84 Aspects

The usage scenario and the associated implications result in requirements for the concepts our QKD-TUI shall explain. The BB84 protocol is not a trivial application of QKD, and the protocol has two different points of view in scientific disciplines (computer science and physics). Understanding it down to its details is far more complex than, first, covered in the chapter 2 and, second, appropriate within the scope of this thesis. For this reason, it is crucial to reduce the totality of these details so that the most important aspects for understanding this protocol are covered and, in parallel, the target audience of the usage scenario understands all of the information. Furthermore, the limitation helps keep the complexity of the final TUI in check.
A comparable example is the *TableTop Horse Race TUI*. The researcher also reduced their explanations to the central terms of neural networks. This TUI and the other TUIs by Raffael et al. are all intended to be introductory to a topic. They abstracted all of them to a certain level, and all have been proven effective in their respective studies [15, 13]. We use this finding as the basis for this QKD-TUI concept, which is why this chapter exists. Using the basics from the chapter 2 and the articles and videos from the chapter 5.3, one can identify patterns which aspects are relevant to explain QKD to laypeople.

1. Qubits What bits are to classic computers, qubits are in quantum computing. They are the smallest unit for quantum computers, the basis for quantum cryptography, and, thus, also the BB84 protocol. As with classical bits, qubits can contain information. A qubit is a two-state quantum system that can be distinguished into two single-meaning states by the act of measurement. A wide variety of quantum particles are suitable as qubits. For simplicity, the thesis is limited to photons since these are standard for QKD in the real world. By specific polarization, the photons are brought into states, to which, then again, one can assign a classical binary system. For the BB84 protocol, one needs altogether four states in two different bases. For example, (0°,90°) and (+45°, -45°), or orthogonal/diagonal bases. A base is then assigned the one and the zero in each case (an example illustrated in the figure 4.3). Thus we can also use qubits as classical memory (see figure 4.2).

Figure 4.4: BB84-Aspects: Parties visual examples

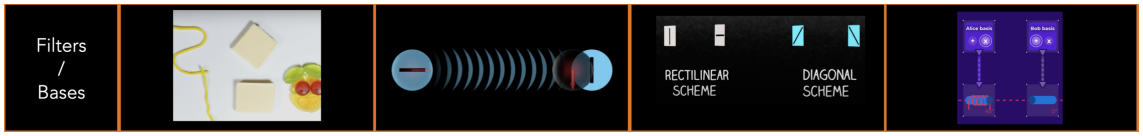


Figure 4.5: BB84-Aspects: Filter/Bases visual examples

2. Parties As with all other protocols, this one also represents a sequence between a certain number of parties. Comparable to other key exchange protocols, the classic parties are *Alice, Bob, and Eve*. We assume that all three have the perfect equipment. We encounter problems such as distance, erroneous transmissions, and measurement errors in the real world. Not only are such things left out in the theory of this protocol, but we also ignore these in the TUI. Since Alice and Bob do not make mistakes, neither does Eve. Latter is standard for any security protocol to assume a maximally dangerous and error-free attack. All three roles are essential components and, thus, a requirement for occurrence in the QKD-TUI. Possible visual representations of these parties one can see in figure 4.4.

3. Filters/Bases Besides 1. mentioning the bases, they are an aspect of their own. They play a crucial role because Alice uses them to send specific information and Bob has to measure Alice's information with the help of the bases. The representation of the bases in other explanation attempts is mostly the same. Typically they use the orthogonal and diagonal bases, but sometimes there are other representations such as right and left and up down (see figure 4.5). Nevertheless, the principle remains the same.

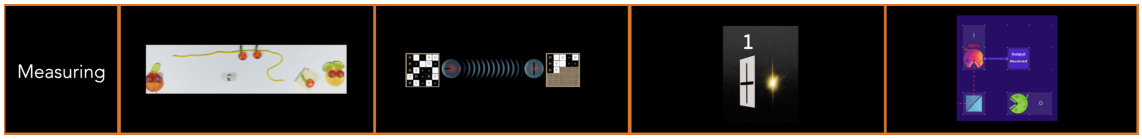


Figure 4.6: BB84-Aspects: Measuring visual examples

Figure 4.7: BB84-Aspects: Public Channel visual examples

4. Measuring The measurement of the photons is as vital as the bases themselves. It must be apparent to the user which outputs the protocol can cause by the different combinations of information sent and bases used for measurement. Eve can influence Bob's measurement. The user must recognize that Eve stands out by measuring and can be discovered in such a way. The underlying physical principles, *Heisenberg's uncertainty principle or the No-Cloning-Theorem*, which guarantees such security, can be deliberately left out because this would distract the attention from the protocol itself. One can see BB84 measuring visualisations in figure 4.6.

5. Public Channel Finally, we have the public channel or the public discussion. This information exchange is a fundamental component of the protocol — both for the key generation and the recognition of Eve. Thus inevitably, for the explanation of the BB84 protocol. The information exchange over the optical channel does not have to be made recognizable as such. Nevertheless, it is essential to understand that the protocol uses two different channels and that the second one can be public without further ado. The exchange of all used bases and the subsequent verification of single bits to detect Eve should be recognizable as two specific steps. One can see BB84 public channel visualisations in figure 4.7.

Aspects as Requirements We intend this chapter's aspects as a minimum requirement for the TUI. The level of detail can deviate from the explanations given here in both directions. The shown figures were also the basis for the co-design workshop. As one can see in chapter 5.2, we also worked together in the workshop on the essential aspects of the participants' opinions. Partly exist an intersection to this section. Regardless of the developed aspects from the workshop, we use these five as a default.

Title	Author	Method	Reference
Tangible Communication of Emotions with a Digital Companion [...]	Jingar et al.	Co-Design	[32]
Co-designing Resources for Ethics Education in HCI	Pillai et al.	Co-Design	[19]
Self-Expression by Design: Co-Designing the ExpressiBall [...]	Wilson et al.	Co-Design	[65]
In the hands of users with Learning Disabilities: Co-Designing [TUIs] [...]	Kanjo et al.	Co-Design	[33]
Itinerarium: Co-designing A Tangible Journey Through History	Marti et al.	Co-Design	[45]
Tangible Cup for Elderly Social Interaction [...]	Bong et al.	CD / FG	[6]
VIC — A [TUI] to train memory skills [...]	Beccaluva et al.	Focus-Group	[4]
EmoBall: a study on a tangible interface to self-report emotional information [...]	Fuentes et al.	Focus-Group	[18]
PLANWELL: Spatial [UI] for Collaborative Petroleum WellPlanning	Nittala et al.	Focus-Group	[50]

Table 5.1: A list of all papers, which we considered relevant regarding the choice of our method.

5 Study Design

This section aims to present how we selected the study method, the course of the study, and how the foundation, a baseline video, was chosen for it. Finally, we describe the selection of the study participants. The goal of the study design was to achieve a result that provides a basis for a design concept for a QKD-TUI.

5.1 Method

First of all, it is clear from the study's objective that we are looking for a method that provides one or some generally held results. We need some selected experts to work together and provide a solution to achieve this. In HCI, two methods are typical for this purpose. One is the focus group, and the other is the more current research method of the co-design workshop (also called co-creation). To find out which method is more suitable, we looked at eight papers from the field of HCI. Four papers used co-design, three used focus groups, and one used both methods. In all papers, a tangible interface was the study's focus. An additional ninth study looked at HCI in learning environments in the context of the ethics behind it [19]. This paper was nevertheless considered despite a deviant focus, as it offers good insights into the co-design workshop method (see Table 5.1).

Focus Group Regarding the studies, a clear pattern exists in which a focus group or a co-design workshop is structured. The focus group usually has two phases. First, the researchers provide information. The latter is an evaluation of previously gathered information, an explanation of the topic and concepts involved, or an introduction to a prototype. Second, the researchers conduct a group discussion. The goal is to gain constructive feedback and valuable insights from the experts' comments. All focus groups from the papers already used a prototype TUI, which is not the case for us [18, 50, 4].

Co-Design Workshop The co-design workshop has three phases. Comparable to the focus groups, a co-design workshop starts with an informative introduction session. The participants, despite their expertise, are provided with the topics' details to grasp the workshop's goal. Afterward, the researchers give the participants a (design-)task in the second phase. The results of this creation session can vary widely. Martin et al. used co-design exercises such as "collages, storyboards, conceptual maps, and paper prototyping" [45]. Kanjo et al. even used real-time 3D printing in addition to story-boarding and drawing to make ideas directly tangible from the workshop participants [33]. Participants in the Jingar et al. study were utterly free to design a TUI with the materials the researchers gave to them. During the exercise, they had "access to the whole lab and personal space for one to free outcome" [32]. In the final phase, the participants present and evaluate their results. For example, in the form of testing, redesigning [45], or self-reflection, where the participants are supposed to use the workshop's insights to take something from it for practice [19].

Decision Since we do not have a prototype yet, the co-design workshop is more suitable than the focus group in our case. Further, the Co-Design studies show ways to actively contribute to the TUI, or in the case of Jinger et al., even to develop new design ideas [32]. The latter is also our goal.
Interestingly, in the study by Bong et al., where they used focus groups and co-design, the focus groups were categorized as part of co-design and would thus be subordinate to co-design [6]. The latter was the only paper that made this categorization without further searching. Furthermore, Kanjo et al. compare co-design and focus groups. They say the "co-design method help make things that are normally unobservable through traditional interviews and focus groups available as resources for design" [33].
We are aware that co-design workshops can be conducted not only with experts but also with the target group. This thesis is deliberately limited to the co-design workshop with experts due to the complexity of the topic. Thus, our chosen method is a co-design workshop. The three phases provided a basis for designing the study guide.

5.2 Study Guide

The three parts of the co-design workshop were *1. Engage & Understand - Introduction Session*, *2. Ideate & Design - Creation Session* and *3. Presentation & Validation (+Feedback)*. The total duration of the study was 90 minutes. The study was conducted twice in the same room with the same conditions. The participants of the two studies came from different backgrounds — more about this in the chapter 5.4.

5.2.1 1. Engage & Understand - Introduction Session

After an initial introduction and naming of the workshop's aim, we started the recording (sound and video). The introduction session consisted of two parts. Part one revolved around TUIs. First, we showed the participants two definitions of TUIs. The first one is a self-created one, and the second one is from the paper by Ishii et al.:

1. A Tangible User Interface is a touchable user interface that allows a computer user to interact with the machine through physical objects. These physical objects contain and implement mechanisms for interactive control and are linked to digital information.

2. TUIs will augment the real physical world by coupling digital information to everyday physical objects and environments. [...] "Tangible Bits" is an attempt to bridge the gap between cyberspace and the physical environment by making digital information (bits) tangible. We are developing ways to make bits accessible through the physical environment [27].

TUIs Then, we showed examples of TUIs and distinguished them based on their form factor. The latter should show that TUIs exist in numerous variations. In addition to the form factor, we showed examples of application areas and explained them (the TUI's function and its intended goal we discussed briefly). The examples were "Breaking barriers expressing emotions" [65], "Understanding forces of nature (physics)" [52], "Workplace support" [28], and "Promoting communication" [53]. Separately, the area of computer science was considered and supported with three examples (PaPl [47], Multithreading TUI [14], Diffie Hellman Key Exchange Protocol (DHKP) TUI [36]). We gave explanations of more specific functionality and purpose for all three TUIs. We particularly emphasized the DHKP TUI since it concerns the cryptographic concept, which pursues a similar goal to this work. First, we explained how the DHKP color analogy works, and afterward, we showed how the designers implemented it in the TUI .

BB84 The second part of the introduction session focused on the BB84 protocol. We selected an explanatory video in advance to bring all participants on a common denominator concerning understanding QKD or the BB84 protocol (see chapter 5.3). Thus, everything explained in the video could be taken as a basis for the further course of the workshop, whether the prior knowledge of individual participants exceeds the information content of the video. After the video, we held a group discussion. The question for group discussion was "*How would you explain the BB84 protocol to someone?*". The idea was that the participants reflect together on the transmitted knowledge and collect all the aspects they consider necessary or have picked up from the video. In parallel, we collected the terms on a whiteboard. We ensured that participants did not draw incorrect information from the exercise or video. We sought a consensus on whether the participants felt everything required was on the board.
Next, we pointed out our selected BB84 aspects (requirements) and explained them. For each column and each picture, we gave a short explanation. This way, we could ensure that these aspects are understandable and appear in the final TUI. We showed many different ways of displaying the images to provide a creative stimulus for session two (see chapter 4.2).

5.2.2 2. Ideate & Design - Creation Session

After a short recap of previously discussed information, we explained the idea of combining a TUI and the BB84 protocol. First of all, we motivated that the BB84 protocol is highly relevant at this time and in the future due to the need for a quantum computer secure key-exchange method. We motivated TUIs on the one hand by their fun factor and the allied increase in motivation. On the other hand, by the scientific evidence that they are particularly well suited to lower entry barriers and thus make complex topics more accessible to people (see chapter 3.5.2).
Next, we divided the groups. In the first study, the six participants built three groups; in the second session, there was one group with three participants. Before starting the creation session, we explained the external presentation scenario to the participants and its implications. The latter provided a framework so that all the groups would be on the same page. Finally, we provided the task: "*Please create an idea or a design concept for a TUI prototype in your group, which is supposed to explain QKD in an external presentation scenario using the BB84 protocol.*"
For this task, all study participants could use the same materials (pens, paper, cards, scissors, sticky notes, glue sticks, tape). We originally scheduled the creation session for 20 min with the option to extend it if needed. The groups needed additional time in both sessions. Nevertheless, both sessions lasted a comparable amount of time (approx. 90 min).

5.2.3 3. Presentation & Validation (+Feedback)

Finally, each group prepared a short final presentation in which they presented their design proposal. For this, they had five minutes. The participants took notes while another group presented to give feedback if necessary. In the first session, there were three presentations and feedback rounds. Finally, the groups reflected on their design based on the feedback and indicated whether they would make any changes or additions. In session two, the feedback round and reflection had to be left out because there was only one group.
After the recording stopped, we offered each participant a study compensation. The Participants could ask questions at any time. Throughout the workshop, we tried to encourage them to ask questions.

#	Article	Language	Source
1	Was ist ein Quantenschlüsselaustausch?	German	[69]
2	Quantenkryptografie – Sicherheit durch Quanteneffekte	German	[77]

Table 5.2: Websources on BB84 Explanation

#	Video name	Language	Duration	Source
1	Quantum Cryptography in 6 Minutes	English	5:57	[81]
2	Quantenkryptografie	German	11:18	[70]
3	Quantum cryptography: Das BB 84 protocol [...]	German	3:44	[78]
4	Quantum cryptography: The BB 84 protocol [...]	English	3:44	[79]
5	Quantum cryptography, animated	None	1:57	[71]
6	Quantum Cryptography Explained	English	8:12	[76]
7	An Uncrackable Code? [...]	English	12:43	[74]
8	What is Quantum Cryptography?	English	12:40	[80]

Table 5.3: Explanation Videos on BB84

5.3 Baseline Video Selection

In order to find out which aspects from the BB84 protocol are essential, we have to look at how others have explained BB84 so far. Since, in the selected scenario, one must assume that the explanation should also be understandable for a layperson, we limit ourselves to simplified explanations and already existing metaphors, which are accessible to non-experts. That means complex explanations like the scientific publications, other scientific articles, lecture slides, or university texts are unsuitable. The keyword search for *Quantum Key Distribution*, *QKD*, *BB84*, and combinations of these provided two scientific articles and eight explanatory videos (German and English) that were considered a basis for the question of relevant aspects. All ten sources are explained in simple language and are easy to understand (see Table 5.2 and 5.3).
Seven sources introduce the topic and motivate either Quantum Cryptography or QKD. The web sources differ from the videos. The web source one [69] starts directly with a general explanation of what QKD is. Using the term quantum key exchange, they infer properties of quantum mechanics that help provide two parties with a total accident number that they can use as a key. They motivate by real examples of QKD applications. At web source two [77], the general importance of encryption, e.g., banks, draws attention to the topic. About the first encryption method, the Enigma decryption, they jump to the current encryption and an explanation of the One Time Pad. The focus is on symmetric encryption and the threat posed by Eve. They introduce QKD by asking about a 100% secure system for exchanging a cryptographic key.
The five videos including an introduction, all do it similarly. First, they explain how messages can be encrypted using cryptographic methods. Latter varies from a simple example of substitution to an explanation of symmetric encryption to public key distribution ([81], [70], [76], [74], [80]).
With the help of one-way functions and the exploitation of the factorization problem, it is shown by [76] how secure current encryptions like RSA are. So secure that even the most powerful computer, or all the computing power in the world combined, would still not be powerful enough to break such encryption in a reasonable amount of time. All videos refer to the brute force method. They do not consider other possibilities for breaking such encryption. Subsequently, the videos explain that quantum computers could exceed the currently available computing power in the next few years and that algorithms such as RSA would suddenly be breakable in a sufficient time, e.g., hours or even minutes [81]. Therefore, there is a need for a secure solution that cannot be broken even by quantum computers. This motivation then introduces QKD, an encryption method based on physical laws.

We use one of the videos as a baseline for the co-design workshop. This video is to bring all study participants and have a common approach for explaining QKD on which to build. Therefore, all videos were considered regarding their explained aspects to conclude which video is suitable as a baseline for the co-design workshop. There are overlaps in the aspects and the kind of explanation. This thesis uses *Video #8: What is Quantum Cryptography?* [80] as a baseline video for the following reasons. Compared to the other videos, video eight introduces the topic and motivates quantum cryptography, and it explains the checkup for Eve via a comparison of a bit subset. Further, it explains Eve sufficiently by introducing her separately. Lastly, the video is in English, thereby understandable to more people, and has an appropriate level of abstraction.

5.4 Participant Selection

From the chapter 5.1, it is clear that we wanted to invite experts, or at least participants with some prior knowledge, for our study. Our planned QKD-TUI combines two scientific disciplines, physics, and computer science. Therefore, the study was conducted twice, with participants from the respective fields.
We recruited the participants from the field of (media) computer science with the help of a study tender. For this purpose, we used channels such as email distribution lists, Slack groups, Discord chats, or University external messenger app groups. The invitation text included a short study description, the location, the approximate time, the type of compensation, and the information that specific prior knowledge in HCI and quantum computing, or quantum key exchange, is required. A link to a short questionnaire in the invitation ensured a certain prior knowledge level. That way, we could screen participants if necessary. At the end of the questionnaire, with the help of a schedule planner, the participants could indicate their preferred workshop dates. After selecting and evaluating the date intersection, all selected participants were sent an email with the final date and confirmation for participation in the workshop. In addition, we have asked the participants to reconfirm. The questionnaire contained the following sections:

1. A short description of the study, general information, and a reference to the further procedure.
2. A description of data collection and consent form.
3. Demographic data (age, gender, employment status).
4. ATI - standard questionnaire.
5. Pre-screening questions from the field of HCI and QKD.
6. Questions about expertise in the area of TUIs.
7. Questions about expertise in the area of classic cryptography and the BB84 protocol.
8. Date selection and completion of the questionnaire.

As the second group of participants, we recruited curators from the *Deutsches Museum Munich*. Through email contact and with the help of a scheduler, we conducted the second study with a total of three curators. They are working on the exhibition project “Light and Painting.” In this project, they deal “with the scientific foundations of quantum technology. So [they] approach quantum cryptography more from the physical side” [Participant 1]. Their physics background and experience with exhibits and exhibitions made them the perfect complement to our first round of studies. The curators also completed the questionnaire.
As compensation for the study, we gave all participants the choice of 1.5 HCI points or a 15€ Amazon voucher. The evaluations and results follow in the next chapter.

6 Study Results

Two significant parts divide this Chapter — first, the quantitative questionnaire results, and second the qualitative results of the co-design workshop. The study was conducted twice with participants from different domains and backgrounds. Accordingly, we split the evaluation of the results into these two session (rounds). *R1* represents the first and *R2* the second session. In R1, there were six participants altogether. We divided the workshop into three groups, each with two participants. In R2, there were only three participants who formed one group together. Besides the ATI standard questions, the Likert-scales had seven answer options. For the evaluation, we assigned numbers to the Likert-scale answer as follows:

1. Strongly Disagree (-3 Points)
2. Disagree (-2 Points)
3. Somewhat Disagree (-1 Points)
4. Neither Agree nor Disagree (0 Points)
5. Somewhat Agree (1 Points)
6. Agree (2 Points)
7. Strongly Agree (3 Points)

We evaluated the ATI questionnaire by default but have deliberately assigned negative values to our Likert-scales so that *non-agreements* or *neutral answers* are quickly visible in the evaluation. We calculated the mean, median, and standard deviation whenever possible.

6.1 Questionnaire

6.1.1 Demographics

R1: Of the six participants, five were students, and only one participant worked full-time. All participants have a background in computer science or media computer science. Three participants were male, and three were female. The age median is 23.50 and mean age of the participants is 24.33, with a standard deviation of 1.80.
R2: Of the three participants, two worked full-time, and one was employed part-time. All participants have a background in physics and are curators at the *Deutsches Museum* in Munich. They design exhibitions and are experts in presenting complex topics in exhibitions by making them understandable for museum visitors, especially laypeople. Two participants were female, and one was male. The median regarding age is 36.00, and the mean is 37.33, with a standard deviation of 5.79.

6.1.2 ATI Questions

To be able to order the technical affinity of the participants, we have decided on standard ATI questions. One can take the questions from a ATI standard questionnaire. The calculated average scores per person from R1 were (P1: 4.89), (P2: 5.33), (P3: 4.78), (P4: 5.00), (P5: 4.44), and (P6: 5.33). This results in an overall average of 4.96
In R2 from participants one to three, the averages were (P1: 4.11), (P2: 4.22), and (P3: 4.11), with an overall average of 4.15.
Thus, the participants from R1 are technically more affine than those from R2. The participants from R2 are nevertheless technically affine.

R1	Q1	Q2	Q3	Q4
P1	3	3	3	0
P2	0	0	1	0
P3	1	1	-1	-1
P4	3	3	3	1
P5	2	1	3	1
P6	3	3	3	3
Mean	2.50	2.00	3.00	0.50
Median	2.00	1.83	2.00	0.67
StD	1.15	1.21	1.53	1.25

R2	Q1	Q2	Q3	Q4
P1	1	-2	-2	2
P2	-1	-2	-3	-2
P3	-3	-3	-3	-3
Mean	-1.00	-2.00	-3.00	-2.00
Median	-1.00	-2.33	-2.67	-1.00
StD	1.63	0.47	0.47	2.16

Table 6.1: Pre-Screening HCI Questions - Detailed Answers by Participant and Session

6.1.3 Pre-Screening Questions

We have included pre-screening questions to select participants according to their prior knowledge. We divided the pre-screening questions into the subject area of HCI and QKD. There was a general pre-screening question regarding prior knowledge of the subject. In addition, three detailed questions provided detailed information about the source of the person's expertise.

Pre-Screening HCI Questions We listed the answers of all individual participants in detail in the table 6.1. To keep it brief, we appended all three values (median, mean and standard deviation) to the questions respectively in the following:

1. Q1: I have already dealt with human-computer interaction (HCI) in detail (e.g., attended lectures or read books/specialist articles).
   ($median_{R1} = 2.50$, $mean_{R1} = 2.00$, $std_{R1} = 1.15$, $median_{R2} = -1.00$, $mean_{R2} = -1.00$, $std_{R2} = 1.63$)

2. Q2: I have already read technical literature on the topic of HCI.
   ($median_{R1} = 2.00$, $mean_{R1} = 1.83$, $std_{R1} = 1.21$, $median_{R2} = -2.00$, $mean_{R2} = -2.33$, $std_{R2} = 0.47$)

3. Q3: I have attended a lecture or course on HCI.
   ($median_{R1} = 3.00$, $mean_{R1} = 2.00$, $std_{R1} = 1.53$, $median_{R2} = -3.00$, $mean_{R2} = -2.67$, $std_{R2} = 0.47$)

4. Q4: I have prior knowledge of the topic of HCI from another context.
   ($median_{R1} = 0.50$, $mean_{R1} = 0.67$, $std_{R1} = 1.25$, $median_{R2} = -2.00$, $mean_{R2} = -1.00$, $std_{R2} = 2.16$)

R1	Q1	Q2	Q3	Q4
P1	-2	-2	1	-3
P2	3	3	3	3
P3	3	2	3	3
P4	2	0	1	1
P5	1	1	2	0
P6	-1	1	-3	1
Mean	1.50	1.00	1.50	1.00
Median	1.00	0.83	1.17	0.83
StD	1.91	1.57	2.03	2.03

R2	Q1	Q2	Q3	Q4
P2	2	2	-2	2
P2	3	3	3	3
P3	-3	-3	-3	1
Mean	2.00	2.00	-2.00	2.00
Median	0.67	0.67	-0.67	2.00
StD	2.62	2.62	2.62	0.82

Table 6.2: Pre-Screening QKD Questions - Detailed Answers by Participant and Session

Pre-Screening QKD Questions We listed the answers of all individual participants in detail in the table 6.2. In general, our participants answered the corresponding questions as detailed in the following:

1. Q1: I have already studied the topics of quantum computing (QC) or Quantum Key Distribution (QKD) more intensively (e.g., attended lectures or read books/specialist articles). ($median_{R1} = 1.50$, $mean_{R1} = 1.00$, $std_{R1} = 1.91$, $median_{R2} = 2.00$, $mean_{R2} = 0.67$, $std_{R2} = 2.62$)

2. Q2: I have already read technical literature on QC or QKD. ($median_{R1} = 1.00$, $mean_{R1} = 0.83$, $std_{R1} = 1.57$, $median_{R2} = 2.00$, $mean_{R2} = 0.67$, $std_{R2} = 2.62$)

3. Q3: I have attended a lecture or course on QC or QKD. ($median_{R1} = 1.50$, $mean_{R1} = 1.17$, $std_{R1} = 2.03$, $median_{R2} = -2.00$, $mean_{R2} = -0.67$, $std_{R2} = 2.62$)

4. Q4: I have prior knowledge of QC or QKD from another context. ($median_{R1} = 1.00$, $mean_{R1} = 0.83$, $std_{R1} = 2.03$, $median_{R2} = 2.00$, $mean_{R2} = 2.00$, $std_{R2} = 0.82$)

R1	Q1	Q2	Q3	Q4
P1	3	3	-3	-3
P2	1	1	0	1
P3	1	1	-2	-2
P4	3	0	-3	-3
P5	2	2	-2	-2
P6	3	3	1	1
Mean	2.50	1.50	-2.00	-2.00
Median	2.17	1.67	-1.50	-1.33
StD	0.90	1.11	1.50	1.70

R2	Q1	Q2	Q3	Q4
P2	3	3	2	1
P2	-1	0	0	-2
P3	1	2	-3	-3
Mean	1.00	2.00	0.00	-2.00
Median	1.00	1.67	-0.33	-1.33
StD	1.63	1.25	2.05	1.70

Table 6.3: Detailed TUI Questions - Detailed Answers by Participant and Session

6.1.4 Detailed Questions

Finally, we asked questions on the specific topics of TUI and classic cryptography/BB84. The aim was to determine to what extent the participants had already dealt with the specific sub-areas (beyond the general topics of HCI and QKD) TUI and classic cryptography/BB84.
These questions were not decisive for the invitation to the workshop but should provide a general overview of how detailed the participants' expertise was.

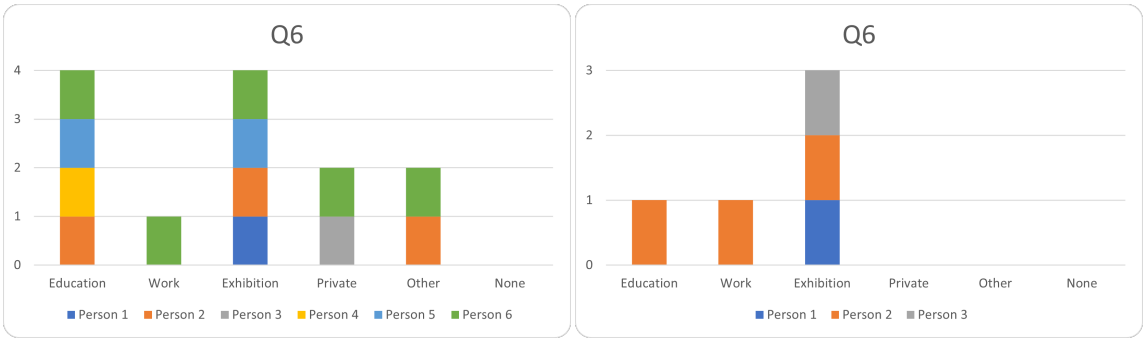
Detailed TUI Questions We listed the answers of all individual participants in detail in the table 6.3. In general, our participants answered the corresponding questions as detailed in the following:

1. Q1: I can clearly imagine what a Tangible User Interface is.
   ($median_{R1} = 2.50$, $mean_{R1} = 2.17$, $std_{R1} = 0.90$, $median_{R2} = 1.00$, $mean_{R2} = 1.00$, $std_{R2} = 1.63$)

2. Q2: I have used a TUI before.
   ($median_{R1} = 1.50$, $mean_{R1} = 1.67$, $std_{R1} = 1.11$, $median_{R2} = 2.00$, $mean_{R2} = 1.67$, $std_{R2} = 1.25$)

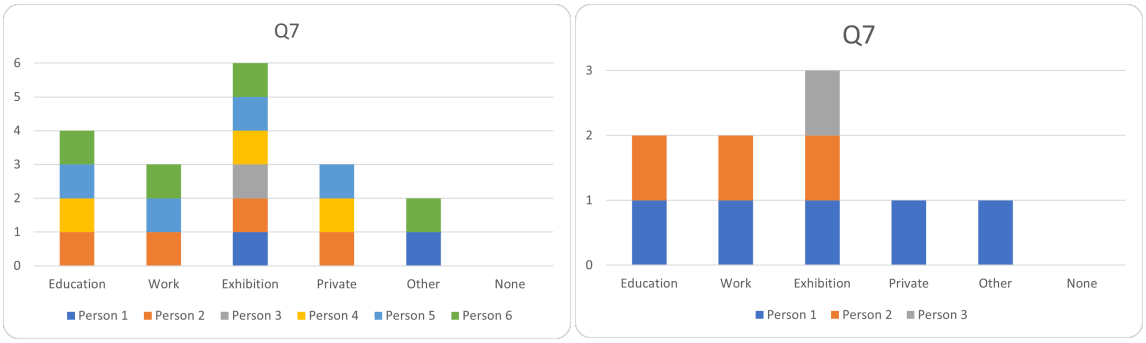
3. Q3: I have designed a TUI before.
   ($median_{R1} = -2.00$, $mean_{R1} = -1.50$, $std_{R1} = 1.50$, $median_{R2} = 0.00$, $mean_{R2} = -0.33$, $std_{R2} = 2.05$)

4. Q4: I have built a TUI before.
   ($median_{R1} = -2.00$, $mean_{R1} = -1.33$, $std_{R1} = 1.70$, $median_{R2} = -2.00$, $mean_{R2} = -1.33$, $std_{R2} = 1.70$)



(a) R1 (b) R2

Figure 6.1: Q6: I have dealt with a TUI in these contexts before.



(a) R1 (b) R2

Figure 6.2: Q7: I can imagine using a TUI to explain an issue in these contexts.

Q5: *How many different TUIs are you familiar with?*: For R1, the participant's responses were from one to six in the same order (2), (2), (2), (3), (2), and (5). The latter results in a median of 2 and a mean of 2.67 with a standard deviation of 1.11.
For R2, the responses of participants from one to three were in the same order (100), (0), and (0). The latter results in a median of 0 and a mean of 33.33 with a standard deviation of 47.14.

Q6: *I have dealt with a TUI in these contexts before.*: In R1, most participants already dealt with a TUI in the context of an *exhibition* or *education*. *Exhibition* and *education* each received four votes from six participants. The context *private* and *other* got two votes, *work* one and *none* zero votes. In R2 the context *exhibition* got three out of three votes. *Education* and *work* got one vote each and *private*, *other* and *none* got no vote (see figure 6.1).

Q7: *I can imagine using a TUI to explain an issue in these contexts.*: In R1, most participants could imagine using a TUI in the context of an *exhibition*. The *exhibition* got six out of six votes. The context of *education* got four votes, *work* and *private* three each, *other* two and *none* no votes. In R2, three out of three participants could imagine using a TUI in the context of an *exhibition*. Two out of three in the context of *education* and *work*. The contexts *private* and *other* received one vote and the context *none* received no vote (see figure 6.2).

R1	Q1	Q2	Q3	Q4	Q5
P1	1	-1	-3	-3	-3
P2	1	1	3	3	2
P3	2	2	1	3	2
P4	3	1	1	0	0
P5	2	2	2	-1	0
P6	-1	-1	1	-3	-3
Mean	1.50	1.00	1.00	-0.50	0.00
Median	1.33	0.67	0.83	-0.17	-0.33
StD	1.25	1.25	1.86	2.48	2.05

R2	Q1	Q2	Q3	Q4	Q5
P1	3	2	2	2	2
P2	1	1	3	3	3
P3	-1	-1	1	-3	-3
Mean	1.00	1.00	2.00	2.00	2.00
Median	1.00	0.67	2.00	0.67	0.67
StD	1.63	1.25	0.82	2.62	2.62

Table 6.4: Detailed Cryptography and BB84 Questions - Detailed Answers by Participant and Session

Detailed Cryptography and BB84 Questions We listed the answers of all individual participants in detail in the table 6.4. In general, our participants answered the corresponding questions as detailed in the following:

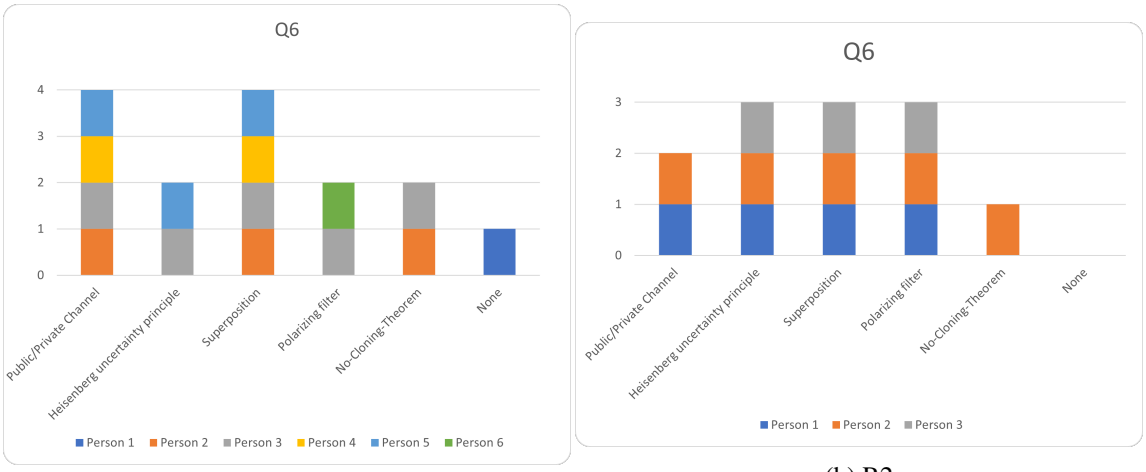
1. Q1: I have already dealt with symmetric/asymmetric cryptographic encryption.
   ($median_{R1} = 1.50$, $mean_{R1} = 1.33$, $std_{R1} = 1.25$, $median_{R2} = 1.00$, $mean_{R2} = 1.00$, $std_{R2} = 1.63$)

2. Q2: I have already dealt with future encryption methods.
   ($median_{R1} = 1.00$, $mean_{R1} = 0.67$, $std_{R1} = 1.25$, $median_{R2} = 1.00$, $mean_{R2} = 0.67$, $std_{R2} = 1.25$)

3. Q3: I have already dealt with Quantum Key Distribution.
   ($median_{R1} = 1.00$, $mean_{R1} = 0.83$, $std_{R1} = 1.86$, $median_{R2} = 2.00$, $mean_{R2} = 2.00$, $std_{R2} = 0.82$)

4. Q4: I have already dealt with protocol BB84.
   ($median_{R1} = -0.50$, $mean_{R1} = -0.17$, $std_{R1} = 2.48$, $median_{R2} = 2.00$, $mean_{R2} = 0.67$, $std_{R2} = 2.62$)

5. Q5: I feel able to explain QKD or the BB84 protocol to a layperson.
   ($median_{R1} = 0.00$, $mean_{R1} = -0.33$, $std_{R1} = 1.05$, $median_{R2} = 2.00$, $mean_{R2} = 0.67$, $std_{R2} = 2.62$)



(a) R1

(b) R2

Figure 6.3: Q6: These topics mean something to me.

Q6: *These topics mean something to me.:* This question was a multiple selection of technical terms in connection with the BB84 protocol or classic cryptography. The choices were *public/private channel*, *Heisenberg uncertainty principle*, *superposition*, *polarizing filter*, *no-cloning theorem*, and *none*.
In R1, the terms *superposition* and *public/private channel* got four out of six votes. The *Heisenberg uncertainty principle*, the *polarizing filter* and the *no-cloning theorem* got two votes each. The selection *none* got one vote.
In R2 the terms *Heisenberg uncertainty principle*, *superposition* and *polarizing filter* got three out of three votes. The term *public/private channel* got two votes and the no *cloning theorem* one. The term *none* got no vote (see figure 6.3).

6.2 Co-Design Workshop

The second part presents the results of the co-design workshop. For this purpose, we have recorded the two workshops with pictures, video, and audio. We then transcribed the recordings. This chapter summarizes the most important aspects.

6.2.1 Aspects for Explaining BB84

First, we look at the group discussion part. Following the baseline video, we asked the participants to work together in a guided group discussion on "which aspects of the BB84 protocol" are essential to explain it to another person. The results were written in parallel on a blackboard using keywords.

R1 The essential aspects for R1 to explain the BB84 protocol were the motivation for the topic, the parties involved, the different spins and filters, the measurement with the bases, the no-cloning theorem, the public channel, and "what the secret key is made of. Namely, of the qubits correctly measured by Bob" [P4].
They wanted to motivate the topic through the "secure key exchange" [P2]. They would introduce Alice and Bob first and then Eve afterward. The public channel is meant for the filter exchange and the check for Eve."[...] but then they talk classically and realize Alice used the same filter as Bob, but the numbers they measured are different, so they know something happened in the middle" [P2] (see figure 6.4).

R2 The essential aspects for R2 to explain the BB84 protocol were the difference between the key and the message, the importance of true randomness, the parties involved, the filters, the polarizers with the polarizations, and the channels.
The curators pointed out that many visitors often lack essential basics, such as the difference between a key and a message. "True randomness, so why do you need it in crypto. Because the idea that you can encrypt securely is something that many visitors think is totally exciting. [...] if you use true randomness, then you can make encryption that is mathematically provably unbreakable. [...] Before the importance of randomness, one must clarify what the message is and what the key is. And that's where I actually had big problems with journalists as well. That was quite difficult. They couldn't imagine it [...]" [P2].
Also, in R2, the participants proposed to explain the protocol first without and then with Eve. In this context, they also said one must clarify how Eve will be detected. They related the latter to the no-cloning theorem. They divided the channels into the optical and "normal" channel.
These aspects complement those from the study design (see figure 6.5). The participants could use them as a basis for their design ideas.

Figure 6.4: MindMap of important aspects for explaining BB84 according to R1

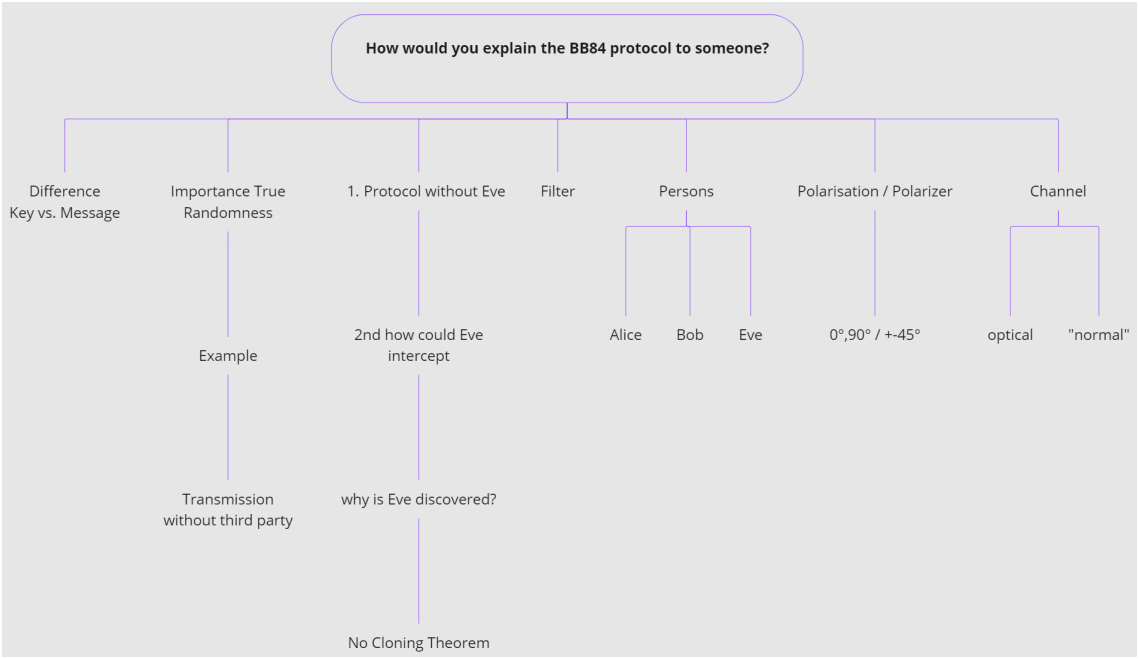


Figure 6.5: MindMap of important aspects for explaining BB84 according to R2

6.2.2 TUI Design Proposals - R1

In session one, the three groups each developed a design idea. Due to the limited workshop time, the three design ideas were only thought through to a certain degree of detail and could not include all aspects.

Group 1 TUI Proposal Group one proposed a TableTop TUI, somewhat reminiscent of an air-hockey table. The TUI is operated by two people, representing Alice and Bob, respectively. Alice and Bob each have gates on their side that contain sensors. These gates are supposed to represent the filters through which the qubits are sent (Alice) or received (Bob). For sending, Alice has small chips/pucks. These pucks are tangible qubits. On one side, there is a one, and on the other side a zero. Alice can now take a puck and choose a side. Alice then chooses which of her two gates (Orthogonal or Diagonal) she wants to send her qubit through.
The qubit is recognized and visualized on display as she sends a chip through the sensor gates. Alice thus keeps the active physical chip. Bob does not see what Alice has chosen through a dividing wall in the middle. On his side, now the digital qubit sent by Alice arrives, and Bob has to decide through which of his two gates (orthogonal or diagonal) he wants to measure the qubit. Bob can not see whether the qubit is a one or a zero. They can repeat this, e.g., ten times. Once one removes the dividing wall, a screen automatically shows which bases each party has used, either for sending (Alice) or measuring (Bob). The match of these bases represents the key. Eve can optionally be added to the interface by a tangible and thus be "activated." A computer automatically simulates Eve. So, as soon as one puts the Eve "hat" in a specific position, the computer recognizes that it should simulate Eve. In doing so, it automatically manipulates the qubits sent by Alice. In the end, Group one did not had time for more details about Eve. However, they then clarified in the subsequent feedback session that the verification of Eve's presence could occur verbally between the two parties and the given information on the display. They also mentioned adding tutorials to the TUI, with essential explanations about context and how it works (see figure 6.6, 6.7 and 6.8).

Figure 6.6: Session 1 - Group 1 - TUI-Proposal with Dividing Wall

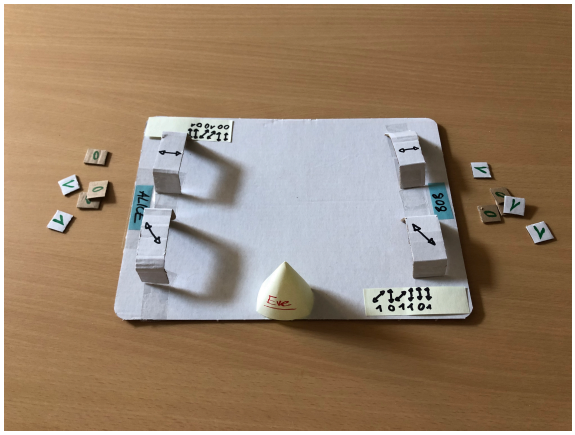


Figure 6.7: Session 1 - Group 1 - TUI-Proposal without Dividing Wall

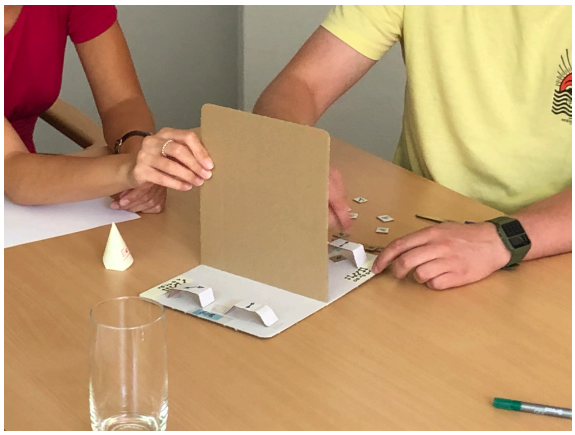


Figure 6.8: Session 1 - Group 1 - TUI-Proposal-Scale

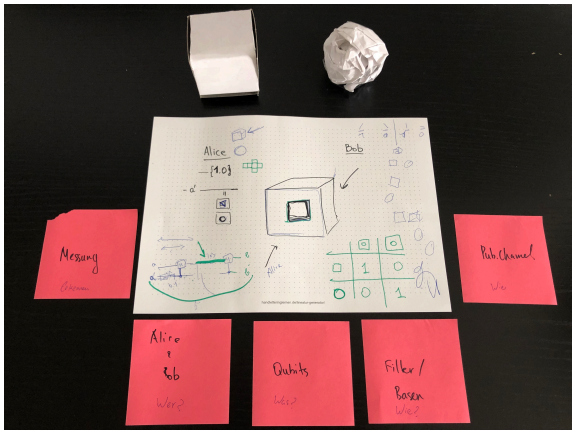


Figure 6.9: Session 1 - Group 2 - TUI-Proposal

Group 2 TUI Proposal Group two proposed a TUI in the form of a box. This box has two sides. So as with group one, two people represent Alice and Bob, respectively. The participants of group two focused heavily on the aspect of qubits. Their idea was to have two filters on each side of the box. One filter is a circle, and the other is a square. Now, with the help of, e.g., Plasticine, which then represents a qubit, one can use the filter-shape to generate either a sphere qubit or a cuboid qubit. The box should then serve as a quantum channel for the transmission. They did not go into further details. Their crucial point then revolve around Bob's measurement. If he measures the Plasticine qubit through the wrong shape (i.e., pushes it through), he gets a wrongly measured result. Latter is only 50% the case in reality, but still crucial for understanding that Bob must use the same filters as Alice. Again, in the subsequent feedback, they mentioned that they would handle the check for Eve via a conversation between the subjects. However, they did not provide information about a functional Eve for their TUI. Whether the Plasticine qubit should be a one or zero could be represented by two different colors. They suggested the latter as an optimization after their presentation (see figure 6.9).

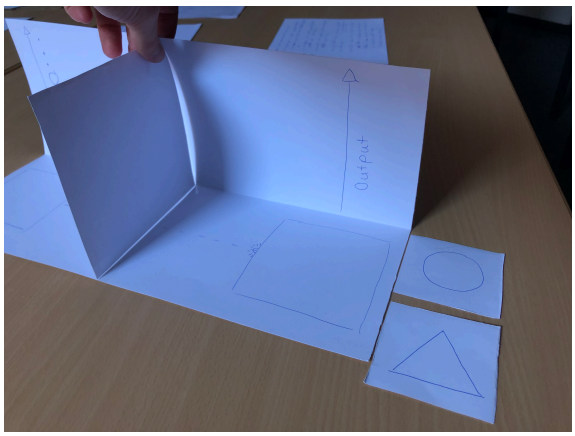


Figure 6.10: Session 1 - Group 3 - TUI-Proposal - with Dividing Wall

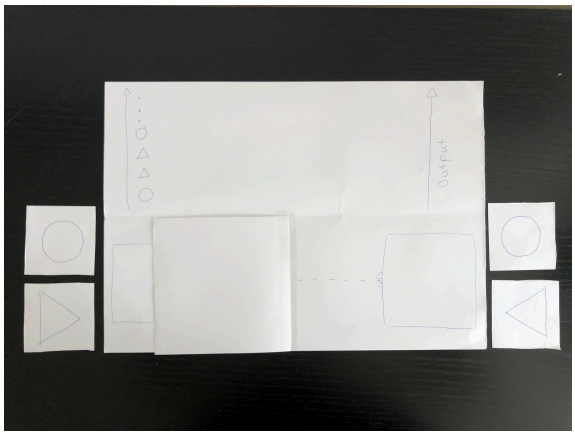


Figure 6.11: Session 1 - Group 3 - TUI-Proposal - without Dividing Wall

Group 3 TUI Proposal Group three also presented a two-people TableTop design with an optional fold-out wall. The latter is to "play" the protocol visible and hidden. However, the TUI is also playable alone since one could take on the role of Alice and Bob by positioning themselves sideways and folding down the wall. The TUI has a screen as "floor" and a screen as "side wall." Alice and Bob each have two blocks representing the filters (a triangle and a circle). Alice puts a block on the screen floor. A sensor recognizes which block is on the floor and sends a digitalized qubit to Bob. Bob receives a sound or light signal, meaning he must also place a block on his sensor for measurement. At the same time, the TUI records on the side panel which bases Alice used for sending and Bob used for measuring. After sending and measuring, the TUI compares the bases and generates a key from the matching blocks. Group three also proposed Eve as a non-controllable element. However, they did not rule out the option of a third person. Then, during the feedback round, group three suggested that Alice have a total of two sensor tiles, one representing the one and the other representing the zero. For Bob, one sensor tile is sufficient, because his two blocks represent the bases *orthogonal* or *diagonal* and he has to choose only one block per qubit, which he then places on his corresponding (one) tile (see figure 6.10 and 6.11).

6.2.3 TUI Design Proposal - R2

The curators proposed a kind of stand-alone machine TUI which is operable by one person taking the role of Bob. The user (Bob) conducts a conversation with Alice via a telephone receiver or a virtual online meeting. Alice is supposed to guide the user through the BB84 protocol since the person using it does not yet know how it works. “Alice says we should exchange a secret message, but we need a secret key for it” [P2]. Over the handset the user can ask questions (or over the virtual meeting the user gets possibly visualized explanations). The user can start the qubit transmission from Alice by pressing a button. They then select, per transmitted qubit from Alice, a filter for measuring with a “rotary wheel”.
The wheel has two possible presets according to the measurement bases. The user can decide per qubit (sent from Alice) in which of the two bases they want to measure. The 1s and 0s resulting from the measurement are essential to generate the key. A legend illustrates how the bases are correlated to the 0s and 1s (see figure 4.3). The user can also discuss this legend with Alice on the phone. They see on display which polarization filters they used and the resulting measurements. After that, a display shows which polarization settings Alice used. In the next step, the user has to choose which polarization settings of Alice matches their own. They select them by pressing buttons. A key is then generated from the selected settings and shown on display. In the last step, again, with the help of Alice, it is clarified that Eve could have been present. Therefore the user randomly picks a subset of the key where they can compare their actively measured bits with Alice hers. The TUI visualizes then any discrepancies on display. Finally, the user has to make a decision. Based on the comparison of the subset, they have to decide if Eve was present and if they want to repeat the protocol or if all went off without a hitch. The TUI resolves then the correct answer. In the case of success, the TUI transmits a message with the generated key.
The curators did not go into more detail about the message transmission. They also did not give further details about Eve. Based on their explanation, we assume that Eve’s presence is random and generated by the TUI (see figure 6.12).

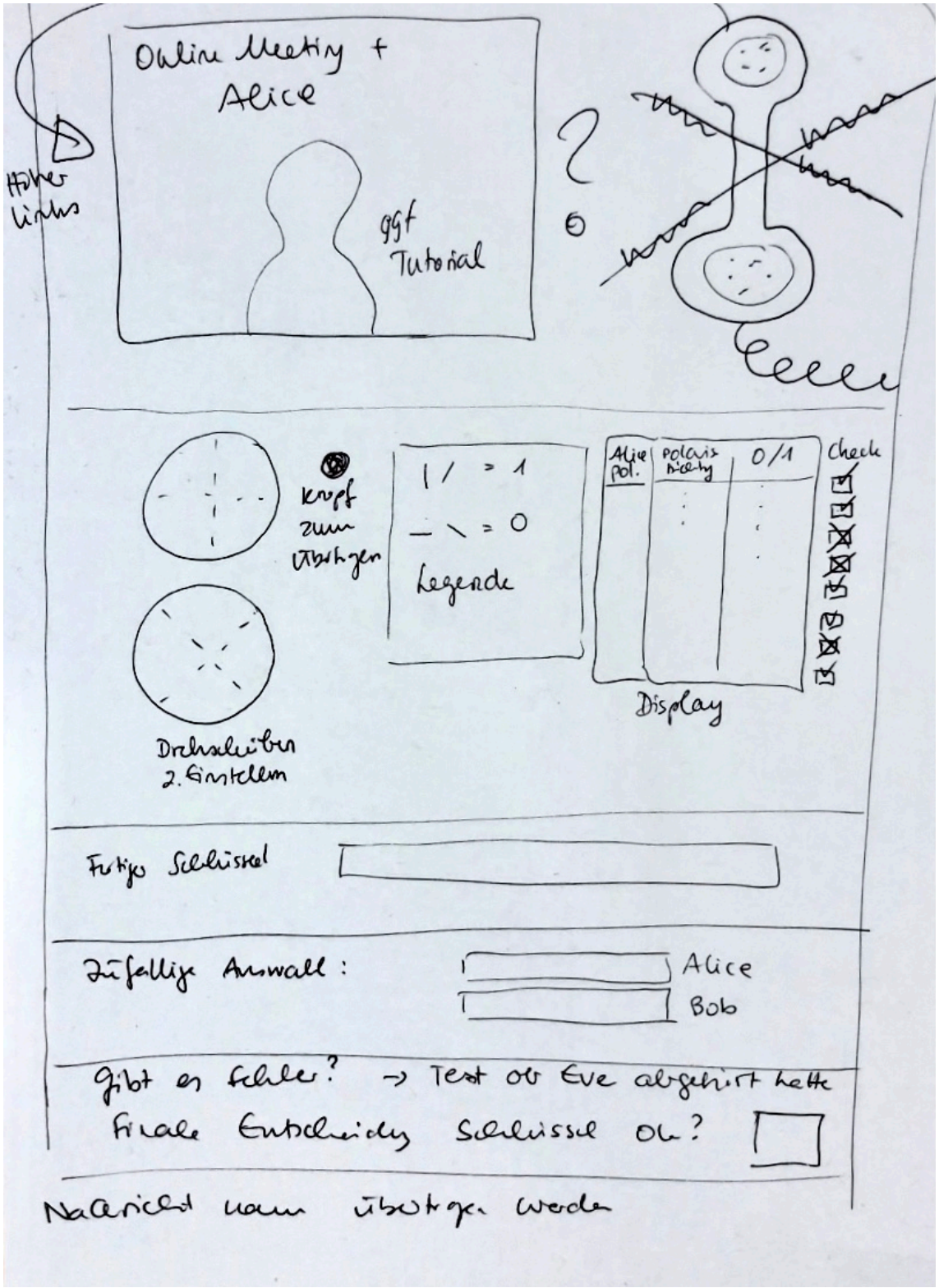


Figure 6.12: Session 2 - TUI-Proposal

7 Limitations and Future Work

This thesis is a conceptual work. We have highlighted aspects from different sciences and tried to combine two elementary topics. This combination of physics, computer science, QKD, and HCI offers much more input than was appropriate in a bachelor thesis. Therefore, we had to limit the scope of this work in some places deliberately. This chapter summarizes the most important limitations and implications for future work.

7.1 Unilateral Related Work

The sixteen papers from chapter 3 all pursued a goal, which they wanted to achieve with the help of a TUI. All were successful in doing so. The TUI performed better in every paper that did a comparison test between the TUI and another technology. In some, it was only marginal but was still considered a success. The latter is maybe because positive results concerning the intended goal are more likely to be published than negative ones. Without a deep research, we did not find any scientific studies in which the TUI performed worse than another technology. In future scientific papers, researchers could actively search for other HCI technologies that performs better than a TUI in explaining complex topics.

7.2 TUI vs. other HCI Technology

These other HCI technologies the researchers could use as the basis for a field test. For example, future work could build a prototype based on this work and then compare it to other HCI learning technologies. To do this, one could invite study participants from the intended target group. With a pre- and post-test on the topic and two different experimental groups, one could then compare the efficiency of the technologies.

7.3 Evaluation of Explanations

In addition, this work did not consider the explanation as such. In Delgado Rodriguez et al.'s survey, we could not verify how the eight QKD experts explained the topic and, more importantly, to what extent these explanations differed. So it could be that their QKD explanations were flawless in themselves but that a misunderstanding arose in the communication at an entirely different point. In future work, we would like to determine more precisely which minimum understanding of basics is necessary for the end user. For this, we propose, a more detailed analysis on the selected external presentation scenario. A concrete definition of the target group could be the first step.

7.4 Building a TUI Prototype

Regardless of the limitations, from our point of view, the next step is to build a QKD-TUI prototype. This thesis can serve as a basis. With the help of user experience design and usability evaluations, the QKD-TUI could be adapted and ultimately tested in an external presentation scenario.

8 Discussion

8.1 Questionnaire

8.1.1 ATI

Generally, the participants from both sessions were technically affine. As expected, the participants from the first session with a computer science background classified themselves as more technically experienced. A proper technical understanding was helpful for the tasks of the co-design workshop but not necessary. For the design of the Tangible User Interface (TUI) proposal, we explicitly pointed out that the participants should not concentrate on technical implementation or details.

8.1.2 Pre Screening

R1: Two participants (2,3) from session one had solid prior knowledge in Quantum Key Distribution (QKD). Interestingly, these two individuals were less adept at the pre-screening questions about Human Computer Interaction (HCI). This finding one can see in reverse for the remaining four participants. Participants one and six had very little prior knowledge of QKD, but they were full experts in the field of HCI. Only participants four and five has some prior QKD knowledge and solid prior knowledge from the field of HCI. Overall, the participants in this session had more knowledge in the area of HCI than QKD, which was nevertheless sufficient.
R2: Participant one had balanced prior knowledge in both areas. Participant two was a full expert in the area of QKD. According to his assessment, he lacked prior knowledge in HCI. Participant three only knew QKD from another context, and she had also no prior knowledge in the area of HCI. We assume that participants two and three were only unfamiliar with the concept of HCI. Nevertheless, through their work as curators, they are implicitly experts in how to design an exhibit and communication. They know how to represent or abstract a complex topic to make it understandable for laypersons. For this reason, participant three was also invited because as a curator, she brings all the requirements for the goal of our workshop.

8.1.3 Detailed Questions

Previous Knowledge on TUIs R1: Four of the six participants had a precise to an exact idea of what a TUI is. These are the same participants who were better versed in HCI than QKD. Participants two and three could imagine what a TUI is, but not as well as the other participants. The results for the usage of a TUI are also comparable. Only participant four took a neutral position. Participant two stated that he had already built a TUI but took a neutral position on the subject of design. Though unlikely, it is within the realm of possibility concerning the other two responses. Participants one, three, four, and five had no experience in designing or building a TUI. Only participant six had experience in design and building a TUI.
R2: Participant one could very well imagine what a TUI is and has already used some. Participant two was less able to imagine a TUI and took a neutral position regarding use and design and an apparent negative position regarding building a TUI. Participant three could somewhat imagine what a TUI is and has used some, but she also took an opposing position regarding the design and building of a TUI. As in the last section, we assume that there was a lack of clarity in the terminology.
The numbers of known TUIs reflects this assumption. Participant one indicated 100 with a "?". Probably because she thought of all exhibits in the *Deutsches Museum*. Participants two and three indicated knowing zero TUIs. During their work, we are sure they were involved with exhibits, one can count as TUI if they are enhanced through digital technologies.
We have asked the participants in which scenario they have already dealt with a TUI and in which

scenario they could imagine using one. R1 & R2: Both in terms of an actual use scenario and a theoretical one, the exhibition performed best in both sessions. Even though the exhibition is not equivalent to our external presentation scenario, parallels are existing. Comparable to the our scenario, it is impossible to foresee what prior knowledge the end user will bring with them in the case of the exhibition. From this, we conclude that all study participants consider a TUI suitable for non-experts end users.

Previous Knowledge on Classic Cryptography and BB84 R1: Participant one has not dealt with future encryption, QKD, or BB84, only with classical cryptography. Accordingly, participant one could not explain the BB84 protocol. Participants four and five already dealt with classic cryptography and had prior knowledge in future encryption and QKD. Participant four referred to the BB84 and the explanation of a neutral position. Participant five has not dealt with the BB84 protocol and takes a neutral position concerning the explanation. Participant 6 has only dealt with QKD. Participants two and three had more expertise in QKD and have already dealt with all topics. They both knew the BB84 protocol well and were confident in explaining it.
In a multiple selection about technical terms, the *public/private channel* and *superposition* scored best. Only participant one was unfamiliar with all terms. However, this is unlikely due to his computer science background and the first choice being *public/private channels*. We assume he put this term in context with the others.
R2: Comparable to participants two and three from R1, participants one and two had prior knowledge in all areas. Participant two's knowledge is more pronounced than from participant one regarding QKD and BB84. Only participant three, comparable to participant six from R1, has only dealt somewhat with QKD.
Concerning the multiple selection of technical terms, one recognizes the physical background that the curators bring with them. *Heisenberg's uncertainty principal*, *superposition*, and *polarization filter* meant something to all of them. Besides the *no-cloning theorem*, these are all terms that exist independently of computer science in physics.

8.2 Co-Design Workshop

8.2.1 Aspects

Both sessions differed strongly from their approach to explain BB84. The latter is visible in the evaluated aspects. In R1, the computer scientists concentrated mainly on the pure protocol itself, and its purpose - the absolute secure key exchange. In contrast, the curators made it clear that for a person who has no prior knowledge, the explanation must be more far-reaching. They explained that, in their experience, the difference between a key and the message itself must be made clear at first. The user must know that "transmitting spins [...] is actually just transmitting the key" [P1]. In addition, according to the curators, explaining the importance of true randomness is also crucial. "If [one] uses true randomness, [one can] make encryption that is mathematically provably unbreakable" [P2]. In their design proposal, Alice takes care of such explanations. However, we also see aspects, which are important to both sessions, such as running the protocol with Alice and Bob first and then bringing Eve into play. The curators focused more on physical correctness. They explicitly mentioned the degrees of the polarized qubits. In contrast, computer scientists only mentioned that there are different spins and alternations of those due to filters.

8.2.2 Proposals

Form All groups (G#) in R1 and R2 proposed a TUI that we classify as at least medium-, if not rather a large-TUI. G1 and G3 from R1 presented TableTops, and in R2, they even proposed a stand-alone machine TUI. Due to its abstract representation, we can not assign the proposal from R1-G2 to a specific dimension. In the chapter 4.2, we specified five indispensable aspects

of the protocol. In order to give each aspect its appropriate attention, a certain amount of space is necessary.
Regarding the external presentation scenario, there is a trade-off. The TUI has to be big enough to give all aspects enough space and small enough so that it remains transportable, especially if one wants to use it at different locations. Future research could find a golden mean for this trade-off through usability testing and user experience design evaluations using a prototype. As a guideline, we suggest that one person should be able to carry the TUI.
The choice of material does not matter at first, but based on our results a display seems to be inevitable in the final TUI. Displays give us the advantage of showing processes and aspects that are difficult to represent as an analog version.

Interaction The two sessions differed most in their interaction with the TUI. In R1, all groups suggested operating the TUI in pairs. Only group three mentioned the possibility of operating the TUI alone. We assume that the DHKP-TUI inspired all groups in R1. The DHKP-TUI also proved that this approach works [36]. However, the curators pointed out that, especially in our external scenario, there is no guarantee that two people will always be available. However, we think it is very likely that, for example, during a visit to the company, at least one person from the team will be available to serve the corresponding counterpart of the TUI.
Nevertheless, the curators decided to use a TUI that is operable alone. Interestingly, the corresponding user takes the role of Bob. An automated Alice explains the problem to him (the user). That way, the curators solved a problem that G1 noticed in R1. G1 admitted that their TUI is not self-explanatory and that they would need a tutorial upfront. Common to all proposals is that the input should be analog, and the output should be digital. We support this approach, so things become tangible that are otherwise inaccessible or intangible, like a qubit.
The two sessions also differ in terms of learning interaction. In R1, all three proposals belong to the *expressive* category of our design space (see chapter 3). The users actively co-create the protocol through their inputs and measurements. Thereby they express their previous understanding of the protocol. In R2, the process is *exploratory*. The TUI guides the user through a prior mental model of the protocol. The users only have to listen to Alice's instructions and execute them. The latter requires less cognitive effort. It may be that with the curators' TUI, the protocol is faster understandable.

Additional Explanations Considering the study of Delgado Rodriguez et al. and the selected usage scenario (external presentation), we are looking for a TUI that supports the understanding of QKD and the BB84 protocol. We can assume that there will always be people in its area of operation which can provide background information or motivation for the topic and, if necessary, operate the TUI themselves. The advantage here is that further explanations are possible during operation.

Budget & Time The proposed stand-alone machine TUI from R2, including Alice's explanations, the possibly built-in Q&A and the visualization of an online meeting, will, in all likelihood, be more complex and time-consuming to build than the proposals of the other session. As a low-fidelity prototype, all suggestions are suitable.

Summary Due to our external presentation scenario, the supporting role of the TUI, and the less complex long-term implementation, we think a design towards the proposals from R1 is more beneficial than the stand-alone machine. Nevertheless, we gained constructive insights from R2, which should be part of the TUI prototype. As a base, two persons shall operate the TUI, representing Alice and Bob. However, in the best case, it should also be operable alone. Here we support the idea of R2 in taking Bob's role and letting Alice guide the user through the protocol. If the latter option is possible, there is a usage scenario beyond the external for the TUI. If otherwise unused, one can place the TUI in a fixed location, so anyone who wants to can use the TUI as Bob. In this case, however, Alice, whom one person otherwise operates, would have to be integrated as a full-fledged simulation. The latter is again a question of budget and time. Further, the idea from R1 to make a qubit tangible differentiates the TUI from other HCI technology and, therefore, is a real advantage.

8.2.3 Additional Design Proposal

As a suggestion, Alice could get a certain number of chips marked with a 1 and 0 (/or are different in color). Alice then can choose whether to throw the 1/0 through an orthogonal-base-slot or a diagonal-base-slot. For example, the TUI recognizes the inserted chip and the used base through a RFID tag. This qubit is now anonymized and sent to Bob, e.g., via a display. Bob uses a wheel inspired by R2s proposal, with predefined base settings to measure the incoming qubit. In parallel, both are shown on a private display what they have measured or sent. After Alice has sent enough qubits, the private display shows all measurement bases from the other person. Both should now decide which parts to keep, e.g., by touch or pressing buttons. As soon as both confirm their selection, whether they match and thus have generated a key is resolved. Eve can be switched on automatically, e.g., by pressing a button. Eve could be visualized by a symbol on display, whether the round is with or without her. Despite a present Eve, whether she is eavesdropping or not is still random. So both parties are forced to discuss a subset of their measured data. They must then decide together whether Eve was present. After the decisions, the TUI shows the correct answer and asks if they want to "play" again.
This proposal is only an example and an inspiration for a possible prototype. Other aspects discussed in the workshops or the thesis are equally valid for a prototype.

9 Conclusion

Due to quantum computers, current encryption algorithms may no longer be secure enough. Post-quantum cryptography is a discipline that aims to protect against this threat even without needing a quantum computer. A sub-discipline of it is Quantum Key Distribution (QKD). The best-known application of QKD is the BB84 protocol, which enables quantum computer secure key exchange. Our goal is to increase the understanding of this sub-discipline. QKD and its application, BB84, should be made accessible to non-experts. In order to teach such complex topics, HCI research relies, among other things, on technology-enhanced learning. Our work has shown that Tangible User Interfaces (TUI) are a promising technology for achieving our goal. This thesis dealt with whether a TUI is suitable to contribute to understanding QKD. With a survey as a basis, we clarified in which usage scenario and for which target group a TUI is useful. We also constructed a co-design workshop to discover what such a TUI could look like.

First, we opened a TUI design space. For this purpose, we analyzed sixteen research papers concerning their TUIs and their fields of application. Despite this technology's very high diversity, we could differentiate them based on characteristics. The chapter 3 divides TUIs into the general form factor, the analog or digital interaction with the user interface, the tangibles as the central TUI element, and finally, the general functionality regarding software and hardware. Sixteen TUIs were used to convey knowledge, i.e., to learn something with the TUIs. We found two different "learning interactions" with a TUI, the *explorative* and the *expressive* interaction. Besides disadvantages like a cost/benefit ratio and the suffering of efficiency/accuracy, we found significantly more positive aspects of learning with a TUI. The two most important insights for the thesis are that TUIs can motivate users and significantly decrease barriers to entry for a complex topic.

Second, we analyzed a suitable scenario for a QKD-TUI using Delgado Rodriguez et al.'s survey. An external presentation scenario is the most suitable. From this, we have derived requirements for the QKD-TUI. QKD or the BB84 protocol must be explainable to an end user without prior knowledge. Inspired by other attempts at explanation, we have defined a minimum requirement for aspects of the BB84 protocol to be in the explanation. These aspects are the *qubits*, the involved *parties*, the *bases/filters*, the *measurement* itself, and the exchange of parties over the *public channel*. The requirements from the scenario and the BB84 aspects became part of our user study.

The goal of our user study was to gather first design ideas for a possible QKD-TUI. For this purpose, we conducted a co-design workshop (twice). The first session was with participants from the field of computer science, and the second was with curators from the *Deutsches Museum Munich*. The curators had a physics background. All participants completed a questionnaire on their suitability for the co-design workshop. In the first session, the participants suitably complemented each other with their intermixed prior knowledge from the field of HCI and QKD. The curators were qualified enough based on their expertise in designing exhibits regardless of the questionnaire.

Especially the comparison of the two sessions of the study produced exciting insights. The computer scientists intensely focused on the protocol itself, while the curators also thought about the basic knowledge requirements. For example, in their experience, some people are unaware of the difference between a key and a message. Further, there is a need to clarify what true randomness is and what advantages it brings to the protocol. One would have to evaluate these findings in further studies with, e.g., with an actual prototype.

In the end, we have gained three design proposals from session one and one from session two. We analyzed and compared concrete aspects of those. These design ideas finally served as inspiration for a design proposal on our part. Our approach is not fully developed in detail and is deliberately not presented as an optimal solution. We only mean to serve as an inspiration for further research in this area and possibly be used as a basis for a concretely implemented QKD-TUI prototype.

References

[1] Mike Ananny. Supporting children's collaborative authoring: Practicing written literacy while composing oral texts. *COMPUTER SUPPORT FOR COLLABORATIVE LEARNING: FOUNDATIONS FOR A CSCL COMMUNITY*, page 595, 2002.

[2] Özgür Anıl, Veli Batdı, and Hüseyin Küçüközer. The Effect of Computer-Supported Education on Student Attitudes: A Meta-Analytical Comparison for the Period 2005-2015. *Educational Sciences: Theory & Practice*, 2018.

[3] Jonny Austin, Howard Baker, Thomas Ball, James Devine, Joe Finney, Peli De Halleux, Steve Hodges, Michał Moskal, and Gareth Stockdale. The bbc micro: bit: from the uk to the world. *Communications of the ACM*, 63(3):62–69, 2020.

[4] Eleonora Beccaluva, Fabiano Riccardi, Mattia Gianotti, Jessica Barbieri, and Franca Garzotto. VIC — A Tangible User Interface to train memory skills in children with Intellectual Disability. *International Journal of Child-Computer Interaction*, 32:100376, June 2022.

[5] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, December 2014.

[6] Way Kiat Bong and Weiqin Chen. Tangible cup for elderly social interaction: Design tui for & with elderly. *Journal on Technology & Persons with Disabilities*, 2019.

[7] M. Born, W. Heisenberg, and P. Jordan. Zur Quantenmechanik. II. *Zeitschrift für Physik*, 35(8-9):557–615, August 1926.

[8] M. Born and P. Jordan. Zur Quantenmechanik. *Zeitschrift für Physik*, 34(1):858–888, December 1925.

[9] Marleny Luque Carbajal and M. Cecília C. Baranauskas. Analyzing the socioenactive dimensions of creative learning environments with preschool children. In *Proceedings of the 19th Brazilian Symposium on Human Factors in Computing Systems*, pages 1–10, Diamantina Brazil, October 2020. ACM.

[10] Alejandro Catala, Javier Jaen, Betsy van Dijk, and Sergi Jordà. Exploring tabletops as an effective tool to foster creativity traits. In *Proceedings of the Sixth International Conference on Tangible, Embedded and Embodied Interaction*, pages 143–150, Kingston Ontario Canada, February 2012. ACM.

[11] Chun-Yen Chang. Does Computer-Assisted Instruction + Problem Solving = Improved Science Outcomes? A Pioneer Study. *The Journal of Educational Research*, 95(3):143–150, January 2002.

[12] Lidong Chen, Dustin Moody, and ,Computer Security Division, National Institute of Standards and Technology, Gaithersburg, MD 20899, USA. New mission and opportunity for mathematics researchers: cryptography in the quantum era. *Advances in Mathematics of Communications*, 14(1):161–169, 2020.

[13] Clifford De Raffaele, Serengul Smith, and Orhan Gemikonakli. Enabling the Effective Teaching and Learning of Advanced Robotics in Higher Education using an Active TUI Framework. In *Proceedings of the 3rd Africa and Middle East Conference on Software Engineering*, pages 7–12, Cairo Egypt, December 2017. ACM.

[14] Clifford De Raffaele, Serengul Smith, and Orhan Gemikonakli. Explaining multi-threaded task scheduling using tangible user interfaces in higher educational contexts. In *2017 IEEE Global Engineering Education Conference (EDUCON)*, pages 1383–1390, Athens, Greece, April 2017. IEEE.

[15] Clifford De Raffaele, Serengul Smith, and Orhan Gemikonakli. An Active Tangible User Interface Framework for Teaching and Learning Artificial Intelligence. In *23rd International Conference on Intelligent User Interfaces*, pages 535–546, Tokyo Japan, March 2018. ACM.

[16] Pierre Dillenbourg, Sanna Järvelä, and Frank Fischer. The Evolution of Research on Computer-Supported Collaborative Learning. In Nicolas Balacheff, Sten Ludvigsen, Ton de Jong, Ard Lazonder, and Sally Barnes, editors, *Technology-Enhanced Learning*, pages 3–19. Springer Netherlands, Dordrecht, 2009.

[17] Randi A. Engle and Faith R. Conant. Guiding Principles for Fostering Productive Disciplinary Engagement: Explaining an Emergent Argument in a Community of Learners Classroom. *Cognition and Instruction*, 20(4):399–483, December 2002.

[18] Carolina Fuentes, Iyubanit Rodríguez, and Valeria Herskovic. EmoBall: A Study on a Tangible Interface to Self-report Emotional Information Considering Digital Competences. In José Bravo, Ramón Hervás, and Vladimir Villarreal, editors, *Ambient Intelligence for Health*, volume 9456, pages 189–200. Springer International Publishing, Cham, 2015. Series Title: Lecture Notes in Computer Science.

[19] Ajit G. Pillai, A. Baki Kocaballi, Tuck Wah Leong, Rafael A. Calvo, Nassim Parvin, Katie Shilton, Jenny Waycott, Casey Fiesler, John C. Havens, and Naseem Ahmadpour. Co-designing resources for ethics education in hci. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI EA '21, New York, NY, USA, 2021. Association for Computing Machinery.

[20] Alexandre Gillet, Michel Sanner, Daniel Stoffler, and Arthur Olson. Tangible Interfaces for Structural Molecular Biology. *Structure*, 13(3):483–491, March 2005.

[21] B.C. Grau. How to Teach Basic Quantum Mechanics to Computer Scientists and Electrical Engineers. *IEEE Transactions on Education*, 47(2):220–226, May 2004.

[22] Roger Hacker and Brian Sova. Initial teacher education: a study of the efficacy of computer mediated courseware delivery in a partnership context. *British Journal of Educational Technology*, 29(4):333–341, October 1998.

[23] Arthur Herman and Idalia Friedson. Quantum computing: how to address the national security risk. *Hudson Institute*, 2018.

[24] Jan Hilgevoord and Jos Uffink. The Uncertainty Principle. *Stanford Encyclopedia of Philosophy*, October 2001. Last Modified: 2016-07-12.

[25] Cindy E. Hmelo-Silver. Problem-Based Learning: What and How Do Students Learn? *Educational Psychology Review*, 16(3):235–266, September 2004.

[26] Michael S. Horn and Robert J. K. Jacob. Designing tangible programming languages for classroom use. In *Proceedings of the 1st international conference on Tangible and embedded interaction - TEI '07*, page 159, Baton Rouge, Louisiana, 2007. ACM Press.

[27] Hiroshi Ishii and Brygg Ullmer. Tangible bits: towards seamless interfaces between people, bits and atoms. In *Proceedings of the ACM SIGCHI Conference on Human factors in computing systems*, pages 234–241, Atlanta Georgia USA, March 1997. ACM.

[28] Robert J. K. Jacob, Hiroshi Ishii, Gian Pangaro, and James Patten. A tangible interface for organizing information using a grid. In *Proceedings of the SIGCHI conference on Human factors in computing systems Changing our world, changing ourselves - CHI '02*, page 339, Minneapolis, Minnesota, USA, 2002. ACM Press.

[29] Heisawn Jeong and Cindy E. Hmelo-Silver. Seven Affordances of Computer-Supported Collaborative Learning: How to Support Collaborative Learning? How Can Technologies Help? *Educational Psychologist*, 51(2):247–265, April 2016.

[30] Heisawn Jeong, Cindy E. Hmelo-Silver, and Kihyun Jo. Ten years of Computer-Supported Collaborative Learning: A meta-analysis of CSCL in STEM education during 2005–2014. *Educational Research Review*, 28:100284, November 2019.

[31] Athanassios Jimoyiannis and Vassilis Komis. Computer simulations in physics teaching and learning: a case study on students' understanding of trajectory motion. *Computers & Education*, 36(2):183–204, February 2001.

[32] Monika Jingar and Helena Lindgren. Tangible communication of emotions with a digital companion for managing stress: An exploratory co-design study. In *Proceedings of the 7th International Conference on Human-Agent Interaction*, HAI '19, page 28–36, New York, NY, USA, 2019. Association for Computing Machinery.

[33] Eiman Kanjo, Kieran Woodward, Gordon Harold, Martin McGinnity, and David Brown. In the hands of users with Learning Disabilities: Co-Designing Tangible Users Interfaces for Mental Wellbeing. *Tangible Interfaces for Wellbeing*, 1 2021.

[34] Fakhreddine Karray, Milad Alemzadeh, Jamil Abou Saleh, and Mo Nours Arab. Human-Computer Interaction: Overview on State of the Art. *International Journal on Smart Sensing and Intelligent Systems*, 1(1):137–159, January 2008.

[35] Ruth Kershner, Neil Mercer, Paul Warwick, and Judith Kleine Staarman. Can the interactive whiteboard support young children's collaborative communication and thinking in classroom science activities? *International Journal of Computer-Supported Collaborative Learning*, 5(4):359–383, December 2010.

[36] M. Fahim Ferdous Khan, Damar Masato Hadisumarto, and Ken Sakamura. A Tangible-Tool-Based Lesson Plan on Cipher Key Exchange Protocol for Early-Stage Learners. In *2022 IEEE Global Engineering Education Conference (EDUCON)*, pages 620–627, Tunis, Tunisia, March 2022. IEEE.

[37] Zachary J. Kirsch and Ming Chow. Quantum Computing: The Risk to Existing Encryption Methods. *undefined*, 2015.

[38] Paul A. Kirschner and Gijsbert Erkens. Cognitive Tools and Mindtools for Collaborative Learning. *Journal of Educational Computing Research*, 35(2):199–209, September 2006.

[39] Agah Tugrul Korucu and Semseddin Gunduz. The effects of computer assisted instruction practices in computer office program course on academic achievements and attitudes toward computer. *Procedia - Social and Behavioral Sciences*, 15:1931–1935, 2011.

[40] Tamer Kutluca and Gülay Ekici. Examining teacher candidates' attitudes and self-efficacy perceptions towards the computer assisted education. *Hacettepe Egitim Dergisi*, pages 177–188, January 2010.

[41] Yanhong Li, Meng Liang, Julian Preissing, Nadine Bachl, Michelle Melina Dutoit, Thomas Weber, Sven Mayer, and Heinrich Hussmann. A Meta-Analysis of Tangible Learning Studies from the TEI Conference. In *Sixteenth International Conference on Tangible, Embedded, and Embodied Interaction*, pages 1–17, Daejeon Republic of Korea, February 2022. ACM.

[42] Thomas G Lynch, David J Steele, Jodi E Johnson Palensky, Naomi L Lacy, and Sean W Duffy. Learning preferences, computer attitudes, and test performance with computer-aided instruction. *The American Journal of Surgery*, 181(4):368–371, April 2001.

[43] Karola Marky and Fachgebiet Telekooperation. *Privacy-Sovereign Interaction*. PhD thesis, Technische Universität Darmstad, 2020.

[44] Paul Marshall. Do tangible interfaces enhance learning? In *Proceedings of the 1st international conference on Tangible and embedded interaction - TEI '07*, page 163, Baton Rouge, Louisiana, 2007. ACM Press.

[45] Patrizia Marti, Michele Tittarelli, and Iolanda Iacono. Itinerarium: Co-designing a tangible journey through history. In *Proceedings of the 9th Nordic Conference on Human-Computer Interaction*, NordiCHI '16, New York, NY, USA, 2016. Association for Computing Machinery.

[46] Juan Mateu and Xavier Alaman. Cubica: An example of mixed reality. *Journal of Universal Computer Science*, 2013.

[47] Aditya Mehrotra, Christian Giang, Noé Duruz, Julien Dedelley, Andrea Mussati, Melissa Skweres, and Francesco Mondada. Introducing a Paper-Based Programming Language for Computing Education in Classrooms. In *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education*, pages 180–186, Trondheim Norway, June 2020. ACM.

[48] David Merrill, Emily Sun, and Jeevan Kalanithi. Sifteo cubes. In *CHI '12 Extended Abstracts on Human Factors in Computing Systems*, pages 1015–1018, Austin Texas USA, May 2012. ACM.

[49] Ananda Mitra and Timothy Steffensmeier. Changes in Student Attitudes and Student Computer Use in a Computer-Enriched Environment. *Journal of Research on Computing in Education*, 32(3):417–433, March 2000.

[50] Aditya Nittala. *PLANWELL: spatial user interface for collaborative petroleum well-planning*. Association for Computing Machinery, November 2015.

[51] Sara Price and Carey Jewitt. A multimodal approach to examining 'embodiment' in tangible learning environments. In *Proceedings of the 7th International Conference on Tangible, Embedded and Embodied Interaction - TEI '13*, page 43, Barcelona, Spain, 2013. ACM Press.

[52] Hayes Solos Raffle, Amanda J. Parkes, and Hiroshi Ishii. Topobo: a constructive assembly system with kinetic memory. In *Proceedings of the 2004 conference on Human factors in computing systems - CHI '04*, pages 647–654, Vienna, Austria, 2004. ACM Press.

[53] Mitchel Resnick, Fred Martin, Robert Berg, Rick Borovoy, Vanessa Colella, Kwin Kramer, and Brian Silverman. Digital Manipulatives: New Toys to Think With, 1998.

[54] R L Rivest, A Shamir, and L Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. In *Secure communications and asymmetric cryptosystems*, page 15, February 1978.

[55] Hong Kian Sam, Abang Ekhsan Abang Othman, and Zaimuarifuddin Shukri Nordin. Computer Self-Efficacy, Computer Anxiety, and Attitudes toward the Internet: A Study among Undergraduates in Unimas. *Journal of Educational Technology & Society*, 8(4):205–219, 2005. Publisher: International Forum of Educational Technology & Society.

[56] You-Jin Seo and Diane Pedrotty Bryant. Analysis of studies of the effects of computer-assisted instruction on the mathematics performance of students with learning disabilities. *Computers & Education*, 53(3):913–928, November 2009.

[57] Orit Shaer and Eva Hornecker. *Tangible User Interfaces: Past, Present and Future Directions*. Now Publishers Inc, 2010. Google-Books-ID: vh_tCfvK4M4C.

[58] Lily Shashaani. Gender-based differences in attitudes toward computers. *Computers & Education*, 20(2):169–181, March 1993.

[59] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, 41(2):303–332, January 1999.

[60] N. J. A. Sloane and Aaron D. Wyner. Communication Theory of Secrecy Systems - The material in this paper appeared originally in a confidential report "A Mathematical Theory of Cryptography" dated Sept. 1, 1945, which has now been declassified. In *Claude E. Shannon*. IEEE, 2009.

[61] Gerry Stahl, Timothy Koschmann, and Daniel Suthers. Computer-Supported Collaborative Learning. In R. Keith Sawyer, editor, *The Cambridge Handbook of the Learning Sciences*, pages 479–500. Cambridge University Press, Cambridge, 2 edition, 2014.

[62] Salih Uşun. Dünyada ve Türkiye'de bilgisayar destekli öğretim. *Ankara: Pegem A Yayıncılık*, 2000.

[63] Gilles Van Assche. *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, Cambridge, 2006.

[64] Stephen Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1):78–88, January 1983.

[65] Cara Wilson, Laurianne Sitbon, Bernd Ploderer, Jeremy Opie, and Margot Brereton. Self-expression by design: Co-designing the expressiball with minimally-verbal children on the autism spectrum. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[66] Kara Zzet and Yakar Harun. Effects of computer supported education on the success of students, 2008.

[67] Salih Çepni, Erol Taş, and Sacit Köse. The effects of computer-assisted material on students' cognitive levels, misconceptions and attitudes towards science. *Computers & Education*, 46(2):192–205, February 2006.

Web-References

[68] Quantencomputer - Erreichte Qubits. https://de.statista.com/statistik/daten/studie/1198694/umfrage/anzahl-der-erreichten-qubits-nach-unternehmen/. Last accessed October 27, 2022.

[69] Quantenschlüsselaustausch: Erklärung, Funktionsweise & Vorteile. https://www.kryptowissen.de/quantenschluesselaustausch.php. Last accessed October 27, 2022.

[70] BYTEthinks. Quantenkryptografie. https://www.youtube.com/watch?v=jrKVdPMc8U4, July 2016. Last accessed October 27, 2022.

[71] Centre for Quantum Technologies. Quantum cryptography, animated. https://www.youtube.com/watch?v=LaLzshIosDk, October 2016. Last accessed October 27, 2022.

[72] Josh Clark. How Quantum Cryptology Works. https://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm, October 2007. Last accessed October 27, 2022.

[73] Tommaso Gagliardoni. Quantum Attack Resource Estimate: Using Shor's Algorithm to Break RSA vs DH/DSA VS ECC. https://research.kudelskisecurity.com/2021/08/24/quantum-attack-resource-estimate-using-shors-algorithm-to-break-rsa-vs-dh-dsa-vs-ec August 2021. Last accessed October 27, 2022.

[74] Munich Center for Quantum Science & Technology. An Uncrackable Code? (Quantum Cryptography) - A Quantum Scientist Explains #QuantumMinutes. https://www.youtube.com/watch?v=y1-vyhpshLc, August 2021. Last accessed October 27, 2022.

[75] Jordan Novet. Google says its quantum computer is more than 100 million times faster than a regular computer chip. https://venturebeat.com/2015/12/08/google-says-its-quantum-computer-is-more-than-100-million-times-faster-than-a-regul December 2015. Last accessed October 27, 2022.

[76] Physics Girl. Quantum Cryptography Explained. https://www.youtube.com/watch?v=UiJiXNEm-Go, March 2016. Last accessed October 27, 2022.

[77] Welt der Physik. Quantenkryptografie – Sicherheit durch Quanteneffekte. https://www.weltderphysik.de/gebiet/technik/quantenmechanik-quantentechnik/quanten-kryptographie/. Last accessed October 27, 2022.

[78] QuantumVisions (WWU Münster). Quantenkryptographie: Das BB 84 Protokoll (U3-02-03). https://www.youtube.com/watch?v=jS0nRbuSBAo, October 2021. Last accessed October 27, 2022.

[79] QuantumVisions (WWU Münster). Quantum cryptography: The BB 84 protocol (U3-02-03). https://www.youtube.com/watch?v=2kdRuqvIaww, October 2021. Last accessed October 27, 2022.

[80] Sabine Hossenfelder. What is Quantum Cryptography? https://www.youtube.com/watch?v=fLJ9mvTS68Y, September 2020. Last accessed October 27, 2022.

[81] Up and Atom. Quantum Cryptography in 6 Minutes. https://www.youtube.com/watch?v=uiiaAJ3c6dM, October 2017. Last accessed October 27, 2022.