The Marb(e)lous BB84: Exploring Tangible Interfaces to Explain Quantum Key Distribution to Adults

SARAH DELGADO RODRIGUEZ✉, University of the Bundeswehr Munich, Germany
KATHARINA BARLAGE, LMU Munich, Germany
ISMAEL PRIETO ROMERO, University of the Bundeswehr Munich, Germany
TIMO WEISBARTH, Enobyte, Germany
LINUS STETTER, LMU Munich, Germany
FLORIAN ALT*, LMU Munich, Germany



Fig. 1. We present *the Marb(e)lous BB84*, a tangible interface that explains the basic principles of Quantum Key Distribution to adults. Using marbles as a tangible representation of qubits (here: photons) – which are impossible to observe with human senses – *the Marb(e)lous BB84* guides two explainees (Alice & Bob) through the steps of the BB84 key-exchange protocol. By designing, implementing, and evaluating our prototype with stakeholders from industry, research, and popular education, we derived insights into the benefits and challenges of applying tangible interfaces for adult cybersecurity education.

We explored the use of tangible interfaces to explain Quantum Key Distribution (QKD) – an inherently complex but increasingly important cybersecurity topic – to adults. Tangible interfaces can support the understanding of complex topics. Yet their role in cybersecurity remains underexplored, despite persistent demands for security awareness and Quantum Computing education. To address this, we applied a participatory approach: (1) exploring current explanations through a survey of QKD professionals ($N = 8$) and analysis of popular YouTube videos, (2) conducting ideation workshops ($N = 9$) to derive design considerations, (3) developing *the Marb(e)lous BB84* educational interface, and (4) comparing its benefits and challenges with slides and the most popular video ($N = 43$). We found that supporting exploration and playfulness is key, as well as rooting explanations in real-world scenarios. Our tangible interface was perceived as highly engaging and attractive. Finally, we contribute design implications for cybersecurity explanation interfaces targeting adults.

*Also with University of the Bundeswehr Munich.

Authors' Contact Information: Sarah Delgado Rodriguez, University of the Bundeswehr Munich, Munich, Germany, sarah.delgado@unibw.de; Katharina Barlage, LMU Munich, Munich, Germany, katharina.barlage@ifi.lmu.de; Ismael Prieto Romero, University of the Bundeswehr Munich, Munich, Germany, ismael.prieto@unibw.de; Timo Weisbarth, Enobyte, Munich, Germany, c-precisionconference@weisbarth.eu; Linus Stetter, LMU Munich, Munich, Germany, linus.stetter@campus.lmu.de; Florian Alt, LMU Munich, Munich, Germany, florian.alt@ifi.lmu.de.



This work is licensed under a Creative Commons Attribution 4.0 International License.
© 2026 Copyright held by the owner/author(s).
ACM 2474-9567/2026/9-ART95
https://doi.org/10.1145/3831971

CCS Concepts: • **Security and privacy → Usability in security and privacy**.

Additional Key Words and Phrases: Quantum Key Distribution, QHCI, BB84, tangible user interface, tangible interface

ACM Reference Format:
Sarah Delgado Rodriguez, Katharina Barlage, Ismael Prieto Romero, Timo Weisbarth, Linus Stetter, and Florian Alt. 2026. The Marb(e)lous BB84: Exploring Tangible Interfaces to Explain Quantum Key Distribution to Adults. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 10, 3, Article 95 (September 2026), 35 pages. https://doi.org/10.1145/3831971

1 INTRODUCTION

In the digital age, rising cyberattacks and their severe financial and personal costs are aggravated by a limited understanding of security concepts. For example, most users of the Signal messaging app fail to properly compare end-to-end encryption keys with conversation partners due to incomplete mental models [83]. Similarly, many users incorrectly assume that biometric authentication sends biometric data to websites, although it is processed locally, leading to mistrust in this method [79]. Such limited understanding often causes insecure behaviors, exposing users to phishing, social engineering, and other threats despite available protections [3, 83, 88, 90]. Traditional cybersecurity training (i.e., lectures or courses) often fails to engage adults or present abstract concepts in an intuitive and memorable way [81].

Tangible interfaces (TIs) offer an alternative: human cognition inherently takes place in the context of the physical world, is supported by offloading cognitive load to physical objects, and is processed through physical actions – an idea described as *embodied cognition* [91]. Hence, by being situated in the physical world, providing materialized representations of otherwise hard or impossible to directly observe phenomena, and supporting tangible interaction, TIs can make abstract ideas concrete and lower entry barriers through physicality and multi-sensory interaction [9, 31, 65, 69]. These benefits are especially relevant for adult cybersecurity education, which involves stakeholders with diverse backgrounds, needs, and priorities (e.g., developers, decision-makers, analysts, end-users [81, 87]), making it indispensable to offer accessible explanations. Such interfaces also provide the unique opportunity to externalize the abstract logical steps, risks, and consequences of cybersecurity, enabling multi-sensorial and embodied reflections.

Tangible interfaces have proven effective in teaching mathematics [72, 96], programming [10], and artificial intelligence [24], yet their potential for cybersecurity education remains underexplored. Findings from other domains may not transfer directly due to unique challenges, such as diverse stakeholders and the multifaceted nature of cybersecurity, which requires considerations of infrastructures, system models, social constructs, attacks, and vulnerabilities [81, 87]. The few existing tangible approaches to cybersecurity explanations are child-focused (e.g., [21, 58]) or analog games without digital augmentation (e.g., [13, 32, 49]). However, children and adults have different cognitive and developmental needs [68] and interact differently with the same TI [84]. Therefore, interfaces designed for children cannot be assumed to work equally well for adults. Since tangible cybersecurity explanation interfaces for adults are scarce, little is known about design requirements, benefits, and challenges.

To address this gap, we focus on a particularly challenging cybersecurity topic: the BB84 Quantum Key Distribution (QKD) protocol. Understanding Quantum Mechanics is vital for future-proof security, given the looming "Q-Day" when Quantum computers may break traditional methods such as RSA. Yet, Quantum Mechanics has proven to be particularly difficult to grasp [43, 60]. We therefore focus on QKD, as it enables "Quantum-safe" communication and, by lying at the intersection of Quantum Mechanics and cybersecurity, maximizes the generality of our findings for explaining abstract security topics. To this end, we conducted a five-step research process guided by the Framework for Innovation [22]. We first surveyed QKD professionals from industry and research (i.e., those who develop, deploy, manage, or study QKD; $N = 8$) and analyzed the 10 most-viewed explanation videos on YouTube to identify current practices, audiences, and tools. These insights informed participatory workshops with students and science museum curators ($N = 9$), where participants

created paper prototypes (i.e., "Magic Machines" [7]) of tangible BB84 explanation interfaces. We then derived design considerations and implemented *the Marb(e)lous BB84*, a ready-to-use TI that guides two explainees ("Alice" and "Bob") through the protocol step by step. Our interface can also serve as a starting point for further education on Quantum Mechanics. Our final study compared *the Marb(e)lous BB84* to a slide-based presentation and a video, measuring the increase in understanding, trust, usability, user experience, and workload. Overall, we answered the research questions:

- **RQ1 – State of the Art:** What approaches do QKD professionals and popular YouTube videos with an educational focus take to explain QKD?
- **RQ2 – Design:** How can a tangible interface be designed to explain the BB84 QKD protocol to adults, based on the requirements of diverse stakeholders (i.e., students, researchers, professionals, and expert educators)?
- **RQ3 – Comparison:** What opportunities and constraints arise from using a tangible interface to learn about the BB84 when compared with conventional slides and an online video?

We found that QKD professionals mainly rely on slides and oral explanations, while popular YouTube videos differ in style and terminology but share a similar structure. Both target audiences with little prior expertise and stress the importance of engagement. Our workshop participants emphasized accessibility, playfulness, and collaboration to support understanding. In our comparison study, *the Marb(e)lous BB84* achieved similar gains in understanding to slides and video, but received higher enjoyment and hedonic quality (i.e., stimulation and novelty) ratings. In addition, we reflect on the design of our interface, the opportunities and challenges of applying TIs when explaining cybersecurity topics, and derive design implications for cybersecurity explanations targeting adults. Our findings can aid Quantum Computing educators, cybersecurity explainers and explainees, and interface designers to create more accessible and engaging explanations of such abstract concepts.

Contribution Statement. We contribute to research on *cybersecurity explanation methods* by:

(1) developing *the Marb(e)lous BB84*, a ready-to-use tangible cybersecurity explanation interface for adults based on both explainers' and explainees' input, collected through an online survey of QKD professionals, YouTube video analysis, participatory design workshops, and iterative involvement of stakeholders.
(2) providing empirically grounded insights into different explanation methods' impact on the understanding and trust in the protocol, their usability, and user experiences by comparing *the Marb(e)lous BB84* to a slide-based presentation and the most popular video ($N = 43$).
(3) reflecting on our participatory design process, the benefits and challenges of using a TI for cybersecurity explanations, and deriving design implications for future cybersecurity explanation interfaces.

2 BACKGROUND & RELATED WORK

Our work builds on prior research on QKD, tangible approaches to cybersecurity, Quantum education, tangible learning interfaces, and publications in the recently emerging field of Quantum HCI (QHCI).

2.1 The BB84 Protocol

The BB84 protocol is named after its inventors C. **B**ennett and G. **B**rassard in 19**84** [15]. It was the first QKD protocol. It is still used in modern hardware, and inspired later protocols such as B92 [14]. The following explanation is based on [35, 43]. BB84 enables two parties to establish a shared secret key while detecting eavesdroppers with near 100% certainty. A QKD key consists of Quantum bits (qubits), typically photons. Any attempt to reveal information about a photon involves a measurement, which may irreversibly change its state. Alice repeatedly prepares photons by secretly choosing a random bit value (0/1) and a random polarization basis (orthogonal + or diagonal x) and sends the photon to Bob. Bob similarly selects a basis to measure each photon.

If their bases match, Bob obtains Alice's value – if not, the result is a random bit. After many repetitions ($N >$ desired key length), both hold lists of chosen bases and values. Alice and Bob then publicly compare their bases and discard all values measured with mismatched bases.

To detect eavesdropping, they compare a random subset of the remaining values over the public channel. Since any measurement by an eavesdropper would disturb some photons, mismatches reveal interception with high probability. If no eavesdropper is detected, the remaining values form their shared symmetric key.

2.2 Quantum and Cybersecurity Education

Effective security adoption requires accessible explanations and supportive socio-technical environments [81]. Frequently observed misunderstandings of cybersecurity mechanisms among end-users, administrators, and even experts can lead to insecure practices or misplaced distrust [1, 2, 5, 25, 77, 79, 83]. Prior work has therefore examined the underlying challenges of communicating complex cybersecurity topics such as Differential Privacy [23, 57, 92], TLS deployments [61], and End-To-End encryption [4]. Formalizing the need for and design dimensions of such cybersecurity explanations, Viganò and Magazzeni [87] propose the Explainable Security paradigm, which covers the "why," "how," "who," "what," "where," and "when" of cybersecurity explanation.

Similarly, recent work in QHCI highlights the need for usable explanatory interfaces that make Quantum concepts accessible to non-experts, identifying educational tools as a core research direction in QHCI [11, 59, 95]. Education on Quantum Computing also directly relates to cybersecurity, as misconceptions about Quantum threats and defenses are common and can distort corresponding decision-making [62]. QKD is considered a suitable starting point for introducing Quantum concepts [36], as it can be explained with minimal mathematical formalism [35, 36] and is already deployed in practice [33]. Correspondingly, prior work has proposed digital Quantum education tools that explain QKD, including Kohnle and Rizzoli's [60] interactive simulations of BB84 and other QKD protocols[1], as well as the online laboratory platform Quantum Flytrap[2] [56].

2.3 Tangible Education Tools

Tangible interfaces (TIs) have been widely explored in education, particularly for children [9, 40, 65]. TIs can foster exploratory learning, spark engagement, lower participation barriers, and support embodied cognition [9, 91]. They are especially promising for representing the otherwise invisible, such as AI processes [24], molecular structures [38], or biochemical processes [41]. Antle and Wise [9] synthesize cognitive perspectives on such TIs in their Tangible Learning Design Framework, including information processing, constructivism, embodied cognition, distributed cognition, and computer-supported collaborative learning.

Recent research has proposed TIs for cybersecurity education. Mills et al. [73] created the *Cyber Funfair*, combining Raspberry Pi devices with LEGO SPIKE kits to demonstrate vulnerabilities in cyber-physical systems. White et al. [89] developed a slot-car racing activity in which participants could hack a scoreboard to understand basic attacks. Closest to our domain, Khan et al. [58] introduced a tangible system using color sensors and LEDs to teach the Diffie–Hellman key exchange[3] through a color-mixing metaphor. Robotic systems have also been leveraged to communicate cybersecurity concepts: social robots have been used to teach children about online safety and privacy [20, 21]. Other works employed robots in computing and cybersecurity camps for high-school students [19, 67, 94]. However, these TIs for cybersecurity education *primarily target children and teens.*

[1] https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-bb84/Quantum_Cryptography.html, last accessed on January 29, 2026

[2] https://lab.quantumflytrap.com/lab/bb84, last accessed on January 29 2026

[3] Diffie–Hellman key exchange [34] enables two parties to generate a shared secret key by publicly exchanging values computed from private exponents. Its security relies on the hardness of the discrete logarithm problem (i.e., similar to RSA), meaning that, under classical computational assumptions, the shared key cannot be feasibly derived from the exchanged public values.

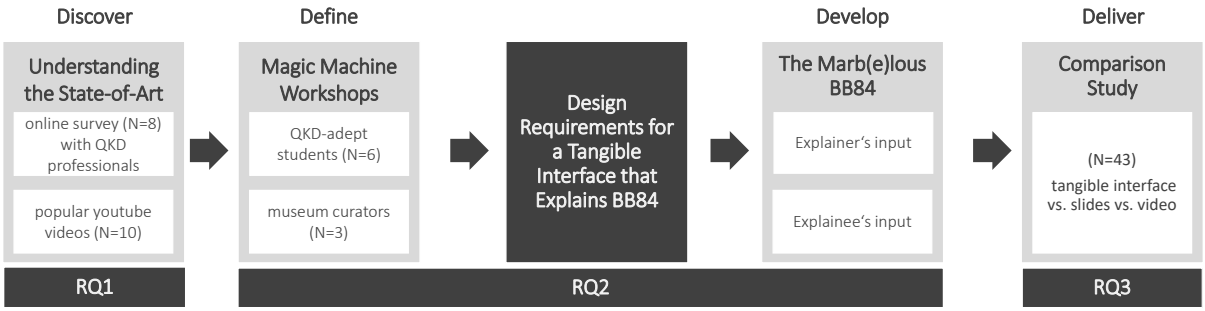


Fig. 2. Using a five-step approach, we investigate the state-of-the-art of QKD explanations for adults, how to design a tangible interface that explains this topic, and the challenges and benefits of such an interface compared to a slide presentation.

Prior work on tangible solutions for adult cybersecurity education has focused on *purely tangible* tools – that is, tools without digital augmentation. Examples include analog games for cybersecurity awareness, such as *Riskio* [49], *Control-Alt-Hack* [32, 93], and various attacker–defender decision games [13, 42, 45]. Examples of *purely tangible approaches to Quantum education* include the game "Entangle me!," a role-play illustrating superposition, entanglement, and decoherence [66], and a "paper strip" model of the knot theory to explain entanglement and gauge symmetries [51].

2.4 Summary & Research Gap

Prior work highlights the importance of explaining cybersecurity to diverse stakeholders, as designers, developers, users, clients, attackers, analysts, and defenders may all find themselves in situations where they need to explain it or receive an explanation [87]. We therefore distinguish between those who explain (*explainers*) and those who receive an explanation (*explainees*). The few existing TIs are designed for children or adolescent explainees, and none target Quantum security. As adults differ from children in their cognitive needs [68] and in the way they interact with TIs [84], it remains unclear how TIs should be designed to support adult cybersecurity understanding.

Hence, there is a clear research gap: adult-oriented TIs for explaining cybersecurity. Our work addresses this gap by introducing a TI that renders otherwise invisible Quantum processes (e.g., photons and measurements) physically graspable for adult explainees, thereby *providing the first investigation of TIs for adult cybersecurity education.* Moreover, QKD is widely considered a suitable starting point for education on Quantum Mechanics [36]. Accordingly, we argue that *the Marb(e)lous BB84* – the TI we developed – not only addresses cybersecurity-related research questions, but also offers a starting point for education in Quantum Computing and Mechanics.

3 RESEARCH APPROACH

Figure 2 shows our systematic research and design process, which follows the UK Design Council's Framework for Innovation [22]. This framework expands the Double Diamond design process by collaborative design principles.

3.1 Double Diamond Design Process

We mapped the Double Diamond design process – which consists of the steps *discover*, *define*, *develop*, and *deliver* – to our research questions in the following manner:

Discover (RQ1 - State of the Art): We answered RQ 1 by *discovering* the current state-of-art [22]. To this end, we surveyed QKD professionals to learn how and in what situations they explain QKD. Moreover, we

analyzed the 10 most-viewed YouTube videos explaining QKD to better understand the content of popular explanations.

Define & Develop (RQ2 - Design): Addressing RQ2, we *defined* potential solutions by conducting participatory workshops to derive design ideas for a tangible interface that explains the BB84 protocol to adults. We then used insights gathered during the first two process phases to derive design considerations for such an interface. Next, we *developed* and iteratively refined *the Marb(e)lous BB84*, which guides explainees step-wise through the BB84 protocol.

Deliver (RQ3 - Comparison): Finally, we *delivered the Marb(e)lous BB84* by evaluating it in a comparison study ($N = 43$) against the current state-of-the-art – a slide presentation and the most popular video (RQ3).

3.2 Application of the Design Principles

The Framework for Innovation also lists four design principles that support an "effective" [22] solution of design problems. We applied them as described in the following:

Put people first. We gathered insights into how and to whom professionals explain QKD and incorporated explainees' perspectives through participatory workshops and iterative user tests.

Communicate visually and inclusively. We introduced all studies and workshops with concise explanations and examples to enable participation independent of prior expertise.

Collaborate and co-create. We involved stakeholders from industry, research, and popular education, using participatory methods to ensure that both explainer's and explainee's needs informed the design early on.

Iterate, iterate, iterate. We continuously incorporated stakeholder feedback to refine the prototype and evaluated the final design to inform future work.

3.3 Ethical Considerations

Low-risk human-subject studies, such as those presented here, are exempt from requiring approval. Hence, the designs of most of our studies were not formally approved by an IRB. Instead, we adhered to our institution's ethical guidelines. In particular, we ensured that participants received a detailed explanation of the data being collected, the purpose of the study, the estimated duration, the compensation, and the voluntary nature of participation, including the option to withdraw at any time before deciding whether to take part in the user study. We also deleted all potentially collected contact, audio, and video data after finalizing the data analysis. Since we had access to the IRB board of a collaborating university at that point, we were able to receive formal approval for the final comparison study under approval number EK-MIS-2025-0433.

4 UNDERSTANDING THE STATE-OF-THE-ART

To answer RQ1, we conducted an online survey targeting QKD professionals and analyzed the content of the ten most popular relevant YouTube videos, as the general population very frequently uses this platform to learn about new topics, and YouTube's view metrics clearly indicate the popularity of different explanations.

4.1 QKD-Professionals Survey

Our online survey investigates how professionals explain QKD. In particular, we explored the contexts in which these explanations occur, the audiences they target, and the tools professionals currently use or wish they had.

4.1.1 Questionnaire Design. The survey started with self-assessments of QKD expertise and experience before asking how often participants had encountered six explanation scenarios: (1) marketing (e.g., promoting a product), (2) external presentations (e.g., trade fairs, visitors), (3) internal settings (within their organization), (4) exhibitions (e.g., museums), (5) teaching, and (6) private conversations (friends, relatives). See Appendix A.1 for details.

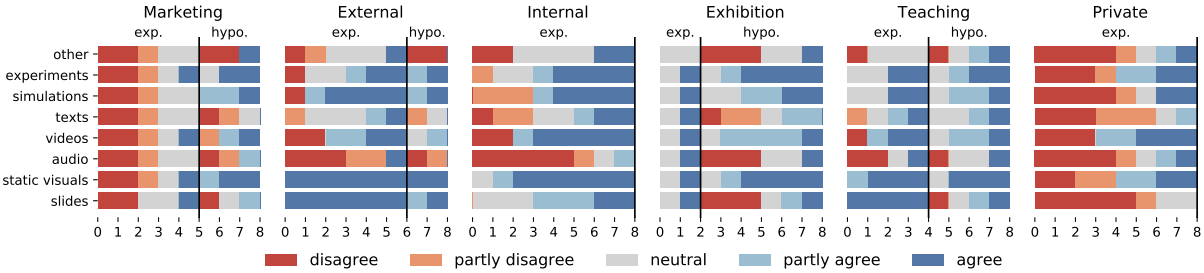


Fig. 3. QKD professionals rated whether they would like to use different tools to explain QKD. We distinguish between participants who have actually experienced each scenario before (exp.) and participants who have not (hypo.)

For each experienced scenario, participants described the audience and assessed its QKD expertise and motivation. They reported which explanatory tools they had used or preferred. For scenarios they had not experienced, participants imagined potential audiences and suitable tools. Finally, participants reflected on the ease of explaining and understanding QKD, the feedback they received, and the need for additional support. Open-ended questions captured perceived challenges, ideal tools, and further comments, followed by demographics.

4.1.2 Data Analysis. We performed descriptive analyses for all Likert-scale, single-choice, and multiple-choice responses. One researcher derived themes from free-text answers. A second researcher revised all findings.

4.1.3 Recruitment & Participants. Answering the questionnaire took about 30 minutes, and participants could enter a raffle for 3x30€. To distribute the survey, we reached out to companies developing QKD hardware and to QKD-related research projects, asking them to distribute it or forward us further contacts. Overall, we contacted 13 different groups. We sent out a reminder a week later, again suggesting that our invitation be distributed more broadly, and finally recruited eight participants. Participants ($N = 8$) were 22-58 years old ($mean = 36.875$, $std = 12.23$) and mostly male (7 males). All participants reported understanding the physical effects on which QKD is based ($mdn = 4.5$) and one or more QKD protocols ($mdn = 5$). They mostly use software to control or monitor QKD hardware ($mdn = 3$, see Appendix A.2).

4.1.4 Limitations. We rely on self-reported data, which may be affected by social desirability and recall bias. Recruiting QKD professionals proved challenging, resulting in a small and predominantly male sample. To preserve participants' anonymity and comply with institutional ethics guidelines, we did not collect information on affiliations or roles, which prevents further analysis of response rates. While prior work found that similarly sized samples provide valuable insights for formative studies [53, 64], the generalizability of our findings remains limited and requires future confirmation.

4.1.5 Results. The following observations are guided by Likert-scale medians and focus on the most important findings. Appendices A.2 and A.3 list all quantitative findings in more detail.

Explanation Experiences. Participants reported that QKD topics are easy to explain, but not easy to understand. Most participants ($N >= 5$) have explained QKD in internal and private contexts at least 6 times. Marketing and external presentation scenarios were less common (mostly 1–5 times), and most participants had no experience in teaching and exhibition scenarios.

Participants reported commonly using slides ($n_{sum} = 17$), no tool at all ($n_{sum} = 13$), static visuals ($n_{sum} = 11$) or texts ($n_{sum} = 7$). Videos ($n_{sum} = 5$), simulations ($n_{sum} = 4$), experiments ($n_{sum} = 3$) and audio ($n_{sum} = 2$) were each used only occasionally. They also indicated using *"exhibition pieces"*, *"demonstrators" QKD hardware*, a *"simulation website"*, *pen and paper for drawing, a whiteboard, and a YouTube video.*

Table 1. We identified the 10 most popular (most viewed) YouTube videos that explain QKD as of September 2024. We excluded shorts, videos that did not provide actual explanations, and non-English videos from our analysis.

	Video Title	**Channel**	URL
1	What is Quantum Cryptography?	Sabine Hossenfelder	https://youtu.be/fLJ9mvTS68Y
2	Quantum Cryptography in 6 Minutes	Up and Atom	https://youtu.be/uiiaAJ3c6dM
3	What is Quantum Cryptography? An Introduction	Eye on Tech	https://youtu.be/_5NQf8k3Jo0
4	How Quantum Key Distribution Works? (BB84 & E91)	Improbable Matter	https://youtu.be/V3WzH2up7Os
5	Quantum Key Distribution Animation	IQC Institute for Quantum Computing	https://youtu.be/cWpqlgF7uEA
6	Quantum Key Distribution, 8884–simply explained | Quant. 1x1	Tüftellab	https://youtu.be/8hNQyTdNil4
7	BB84 Protocol of quantum key distribution	창하김	https://youtu.be/44G9UuB2RWI
8	Quantum cryptography: The BB 84 protocol (U3-02-03)	QuantumVisions	https://youtu.be/2kdRuqvIaww
9	Quantum Key Distribution | QuTech Academy	QuTech Academy	https://youtu.be/lVXJgn3fDkg
10	28.Quantum key distribution I: BB84 protocol	Jochen Rau	https://youtu.be/u_K9jPBrOwA

Desired Tools. In general, participants wished for more tools to support their explanations during external and internal presentations, as well as during teaching (see Figure 3). However, they expressed little desire for additional tools during marketing and private situations. Overall counts of positive ratings (i.e., 4 or 5 values) revealed that participants most frequently preferred static visuals ($N = 36$), videos ($N = 31$), experiments ($N = 28$), simulations ($N = 27$), and slides ($N = 24$). All other tools were selected less frequently ($N <= 13$).

Explainee's Motivation and Expertise. Our participants have explained QKD in the past to visitors, public/industry decision makers, (university) students, experts/collaborators, (business) acquaintances, potential users/developers, colleagues/superiors, and friends/family. They rated explainees' QKD expertise low and their motivation as high. Appendix A.3 shows participants' perceptions of different groups of explainees in more detail.

Explanation Challenges. Participants reported several challenges when explaining QKD. They noted explainees' limited or highly heterogeneous prior knowledge ($N = 5$), difficulties understanding the importance and advantages of QKD ($N = 3$), and the perceived complexity of the topic ($N = 3$). The interdisciplinary nature of QKD, which touches upon physics, mathematics, and computer science, was also described as a challenge ($N = 2$). Finally, some participants indicated that explainees' motivation to engage with QKD may be limited ($N = 2$).

Ideal Explanation Tool. Participants envisioned ideal QKD explanations as interactive, hands-on experiments ($N = 4$), simulations/live demos ($N = 3$), videos or visuals ($N = 3$), slides or posters ($N = 2$), and books ($N = 1$).

4.2 YouTube Video Analysis

According to surveys, YouTube is the most widely used social media platform by U.S. adults, who mostly use it for learning about new topics[4]. Since a large part of the general population relies on YouTube for self-directed learning, we thematically analyzed the most popular videos explaining QKD to capture their content and strategies.

4.2.1 Data Collection & Analysis. To collect a representative sample of the most popular videos explaining QKD, we searched for "Quantum Key Distribution", applied the "Video" filter, and selected the "sort by view count" option. We then selected the ten most popular full-length English videos that explained QKD (i.e., excluding shorts and purely illustrative animations; see Table 1). We downloaded and manually revised all captions. Two researchers independently developed an initial codebook based on two transcripts (≈ 20%), then agreed on a final codebook (see Appendix B), which was applied to all transcripts with iterative discussion of emerging codes.

[4]See https://www.pewresearch.org/internet/fact-sheet/social-media/ and https://www.thinkwithgoogle.com/intl/en-emea/marketing-strategies/video/self-directed-learning-youtube/. Both were last accessed on January 29, 2026

4.2.2 Results: Thematic Analysis. Some videos begin with a motivational example ($N = 4$) before introducing traditional encryption ($N = 3$), followed by Quantum cryptography ($N = 2$), and finally the QKD protocol ($N = 10$). Others start directly with the QKD protocol ($N = 5$). Terminology and assumed prior knowledge varied substantially. Video 1 used accessible examples (e.g., a credit card in a box for encryption), and casual language (*"But here's the thing"*). In contrast, video 10 assumed prior knowledge of terms such as *Pauli-X gate* and *Hadamard gate*. All other videos fell between these extremes. Several videos motivated BB84 through real-world scenarios, including online shopping ($N = 2$), social networks ($N = 2$), and sensitive data (i.e., personal or governmental; video 4), to highlight the need for encryption ($N = 4$). The application of the BB84 protocol was motivated by the limits of classical security based on computational hardness ($N = 3$) and the Q-Day ($N = 4$).

Answering RQ1 - State of the Art

Explanations of QKD are *shaped by assumptions about explainees' prior knowledge*. Explanations, therefore, often rely on *simple terminology*, and frequently *omit deeper Quantum principles*. While slides remain the dominant explanatory tool in practice, professionals expressed a desire for more interactive and visual tools, such as static visuals, videos, experiments, and simulations, to better sustain explainees' motivation and engagement. This reveals a tension in current QKD explanations: explainers recognize motivation as key, yet primarily rely on presentations that do not support exploratory or embodied forms of understanding [9, 91].

5 DESIGN & DEVELOPMENT OF THE MARB(E)LOUS BB84

We structured the design and development of *the Marb(e)lous BB84* using the design space for tangible privacy and security interfaces (TaPSI) [31] as an organizing framework. Specifically, we group design-related observations along its dimensions of *look & feel* and *user interaction*, and complement these with a *content* dimension.

5.1 Participatory Workshops

We elicited visions for tangible interfaces (TIs) that explain QKD through two participatory workshops inspired by Andersen and Wakkary's [7] "Magic Machine Workshops" to encourage a free exploration of design possibilities without material and functionality constraints. The workshops lasted about 90 minutes each.

5.1.1 Method. Our registration survey covered consent, demographics, prior knowledge of QKD, and TIs.

Procedure. After welcoming our participants and encouraging introductions, we started audio and video recording. We then introduced the concept of TIs using extracts from [55] and examples from prior work. To establish a common understanding of the BB84 protocol, participants watched the most viewed QKD explanation video from our analysis (i.e., no. 1 in Table 1). We then asked participants to *discuss how they would explain the BB84 protocol* in the group, while one researcher wrote down all the aspects of the protocol mentioned on a whiteboard. Next, participants formed groups of two or three and *crafted magic machines* (i.e., paper prototypes) representing their vision of a tangible BB84 explanation using basic materials (e.g., pens, paper/cardboard, glue). Each group *presented their magic machine and received feedback* from the others. Presenters were asked to reflect on whether and how they would integrate the input.

Data Collection & Analysis. Recordings were transcribed, handwritten notes digitized, and all materials consolidated. Two researchers familiarized themselves with all the data, and one researcher then described all prototypes and thematically analyzed participants' input and prototypes, identifying common themes. The second researcher reviewed and refined both the descriptions and themes. Hence, inspired by Braun and Clarke [16, 17], our approach iteratively refined shared observations. Quantitative questionnaire responses were analyzed descriptively.

Recruitment & Participants. Participation required basic QKD knowledge to focus the workshops on design rather than instruction. We recruited students from a Quantum Computing lecture for Session 1 and museum curators involved in quantum-related exhibitions at the Deutsches Museum, a large science museum, for Session 2. All participants were recruited via email and received 15€. Five university students and one PhD student took part in session 1 (3 male, 3 female). They were young adults ($mean = 24.33$, $std = 1.80$) with a high affinity for technology [39] (ATI=4.96). Session 2 included three museum curators (two male, one female), who were older ($mean = 37.33$, $std = 5.79$) and reported a slightly lower ATI (4.15). Participants reported prior experience with Quantum Computing or QKD, but rated their familiarity with BB84 as neutral (Appendix D.1). They were familiar with TIs through prior use, but had not previously designed or built one. Participants had encountered TIs in exhibition ($N = 7$) or educational contexts ($N = 5$).

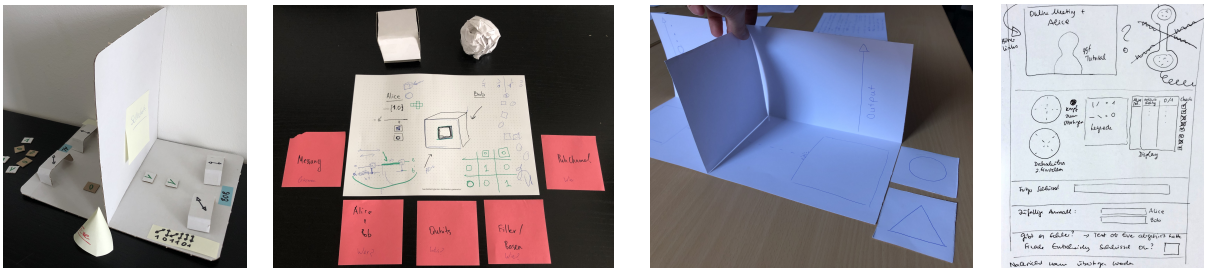
Limitations. As we again relied on self-reported data, our findings may be prone to social desirability and recall bias. Moreover, our sample was small and comprised relatively young participants, which may limit the generalizability of our findings to other populations. We also specifically recruited participants with prior knowledge of Quantum Computing or Quantum Mechanics to focus on developing design ideas rather than starting from scratch by explaining QKD. While our student participants had only recently attended an introductory lecture on Quantum Computing, which may have allowed them to reflect on challenges of initial understanding, our choice prioritizes prior knowledge over representativeness of first-time learners and thus limits the corresponding ecological validity of our findings. Hence, novice participants might have provided additional or different input.

5.1.2 Results.

Content. We asked our participants which aspects of the BB84 protocol are essential to explain. They mentioned the motivation for using QKD (i.e., the desire to exchange a secret message and shared cryptographic keys) and the involved parties (i.e., Alice, Bob, and Eve). They suggested introducing Alice and Bob first and Eve later so the explainees would *"[...] realize Alice used the same filter as Bob, but the numbers they measured are different, so they know something happened in the middle"* [P2, students]. The museum curator particularly highlighted the importance of pointing out the difference between a key and a message: *"[...] one must clarify what the message is and what the key is. And that is where I actually had big problems with journalists as well. That was quite difficult. They could not imagine it [...]"* [P2, curators]. Moreover, participants mentioned explaining qubits, their values, the different bases (or polarization filters), and that the key consists of the qubit's values. They suggested avoiding the terms filters, polarizations, and spins and instead using values and bases, as these would be perceived as less complex. Explainees should also learn how the measured value depends on the chosen base, the no-cloning theorem (without using the specific term), how an eavesdropper might affect the photons' state, and the steps necessary to detect an eavesdropper. Participants also mentioned the need to clearly indicate which parts of the communication are public and which are secret.

Look & Feel. Figure 4 shows all machines crafted by our participants (see also Appendix D.2 for descriptions). All groups envisioned large table-like or tabletop interfaces. Most groups proposed a two-user TI with Alice and Bob, often separated by a privacy screen that prevents each user from seeing the other's actions. Eve was either simulated by the system or introduced as an optional third person.

User Interaction. Several groups suggested exchanging physical objects to represent photons. This was often envisioned in a playful manner (i.e., similar to air hockey, with photons made of plasticine or building blocks). Bases were represented by pairs of gates or holes in two groups, while Group 4 used a rotary wheel. User input was usually tangible or voice-based, and system output (instructions, bases, values, or key information) was shown on displays.



(a) Airhockey (G1) (b) Puzzle Box (G2) (c) Geometric Blocks (G3) (d) QKD Call (G4)

Fig. 4. Each workshop participant group (G) developed one *magic machine* for a tangible interface that explains the BB84 protocol using basic crafting materials (e.g., paper, cardboard, pens, and glue).

5.2 Design Considerations For Tangible Interfaces that Explain the BB84 Protocol

We translated insights from the professional survey, video analysis, and participatory workshops into *design considerations for a TI explaining the BB84 protocol*. We again organized the considerations along the dimensions of *look & feel*, *user interaction*, and *content*, and related them to the Tangible Learning Design Framework (TLDF) [9], situating them in established theories of tangible learning. The TLDF Guidelines are listed in Table 3.

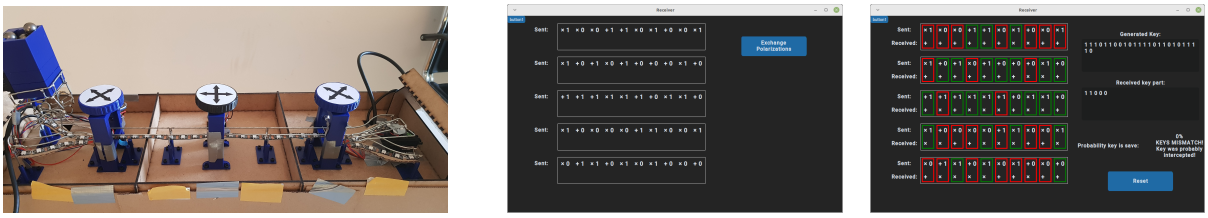
5.2.1 Look & Feel. Participants envisioned *table-like or table-top interfaces*, well-suited for collaboration [10, 96] and attracting bystanders. As explanations occur in diverging contexts, the *interface should remain transportable. Tangible proxies* make invisible photons, their values and bases perceivable. A *privacy screen* indicates which protocol steps are public or secret. Making abstract elements and processes perceptible in this way may support information processing (G2) and the distribution of cognition (G8, G9). As motivation for explainees can vary, participants and professionals proposed *playful, visually appealing designs to foster engagement.*

5.2.2 User Interaction. Workshop participants envisioned *interfaces controlled through direct tangible interaction (i.e., rotation and movement), with feedback provided digitally on displays*, which may leverage embodied cognition (G5 - G7). They support *collaborative use by two explainees representing Alice and Bob*, relating to computer-supported collaborative learning (G10, G11). Participants suggested *hands-on exploration, stepwise guidance, and allowing explainees to test actions and observe effects.*

5.2.3 Content. Videos and workshop input suggest introducing *Alice and Bob (i.e., as human actors) from the beginning, adding Eve later. Explanations should be situated in a relatable real-world scenario,* (e.g., exchanging secret messages), which relates to constructivist theories emphasizing authentic tasks and meaningful goals (G3). Videos and workshop findings also indicate *a preference for simpler terms (i.e., terms that might be known from other contexts, such as bases and values instead of spins or polarization filters)* to reduce perceived complexity. Curators stressed conveying that *BB84 enables key exchange only* and clearly *distinguish public from secret information.*

5.3 Iterative Development Process

Based on our design considerations, we proposed a playful marble track where two explainees exchange tangible photons (marbles). Released marbles pass through “base gates” for Alice, Bob, and Eve. Each gate has a rotary knob to select the measurement base, and the marble dispensers set the qubit’s value. Identical marbles reflect photons’ indistinguishability before measurement. A privacy shield ensures explainees can only see their gate.



(a) Initial Physical Prototype

(b) Initial Graphical User Interface (GUI)

Fig. 5. We implemented a first version of our prototype and then invited three students to test it and provide feedback.

5.3.1 Explainers I: Early Conceptual Feedback. We presented a 3D model of our vision to two QKD researchers to elicit early feedback (see Appendix E.1). They recommended assigning fixed roles (Alice as sender, Bob as receiver) to reduce complexity. They also suggested releasing marbles onto subtracks for values 0 or 1, which merge after leaving Alice to represent indistinguishability, and split again at Bob's side to reflect measured values.

5.3.2 Initial Prototype. Building on this, we implemented an initial version of *the Marb(e)lous BB84* (see Figure 5).

Look & Feel. The prototype combined a laser-cut wooden casing with 3D-printed components, metallic marbles, and metal wire tracks. LEDs highlighted marble movement and selected bases. A servo redirects marbles to value-specific subtracks on Bob's side. Padlock-shaped privacy screens concealed Eve and referenced encryption-related metaphors [29]. A Raspberry Pi and a Raspberry Pi Pico controlled all electronic components.

User Interaction. Both users had a touchscreen. The GUI prompted users to select bases and send photons while displaying chosen bases and values (see Figure 5b, left). After exchanging some marbles, a button appears to proceed to the following steps of the protocol. Matching and mismatching bases were visually highlighted in color (matches in green, mismatches in red). Potential eavesdropping was indicated through a textual message (see Figure 5b, right).

5.3.3 Explainees: First Tests & Refining the Content. We invited three participants with no background in cryptography or prior knowledge of BB84 to test our initial prototype. Each participant completed the test individually. They first acted as Alice, exchanging 10 qubits to complete the key exchange, and then repeated the procedure as Bob. A researcher explained each GUI step and its purpose. Based on participant feedback, we iteratively refined this explanation and used it to inform the final version of *the Marb(e)lous BB84*. All three participants enjoyed interacting with the prototype and felt it improved their understanding of BB84. For improvements, they suggested:

- avoiding distracting references to classical key exchange algorithms (e.g., Diffie–Hellman),
- focusing on key aspects without physics details,
- clearly introducing the eavesdropper (Eve) and their impact,
- improving hardware reliability (e.g., IR sensors, marble movements, and motors).

5.3.4 Refinement. We incorporated this input and the refined explanation script into our physical setup and GUI.

Look & Feel. We replaced the cardboard privacy screens with a padlock-shaped tunnel that more effectively concealed Eve from different viewpoints (see Figure 1). We added a base plate with height-adjustable feet and an integrated spirit level to ensure reliable marble movement. To improve detection and switching reliability, we replaced IR gates with inductive sensors (TL-W5MC1) and substituted the servo motor with a solenoid. We also updated the color scheme, fonts, and graphical elements to enhance the GUI's visual appeal (Figure 6).

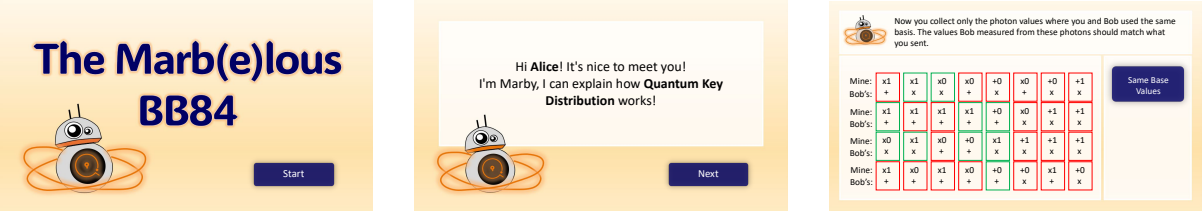


Fig. 6. "Marby" explains the BB84 protocol step-by-step in the final GUI. These screenshots show the start screen (left), the first *explanation screen* which starts the introduction (middle), and a *protocol screen* showing the base comparison (right).

User Interaction & Content. We added an on-screen character named "Marby"[5], who guides explainees through the protocol step by step. Informed by our design considerations and tester feedback, the explanation introduces a scenario in which Alice wants to send a secret message to Bob. It omits distracting terminology and additional topics (e.g., Diffie–Hellman or underlying physics). Users first complete the key exchange without Eve and then repeat the procedure with Eve revealed (i.e., without the privacy screen). To verify correctness and clarity, we shared GUI screenshots with two additional QKD researchers, who suggested minor textual revisions.

5.4 Final Prototype: The Marb(e)lous BB84

Tangible Interface. Figure 7 shows the final version of *the Marb(e)lous BB84* and its components. To sum up, *the Marb(e)lous BB84* has a laser-cut wooden casing that protects and hides the wiring, the computational device (i.e., Raspberry Pi 3), and most electronic components. The Raspberry Pi reproduces the GUI, controls all sensors and actuators, and performs all computational operations. In particular, we designed a PCB shield for the Raspberry Pi, which includes the required connections for all sensors and actuators, such as level shifters and drivers for the solenoid and LED strip. We wrote Python scripts for this purpose and used PyQt to implement the GUI. To prevent overheating, we also installed two fans. The casing is attached to a wooden base plate with height-adjustable feet. Two touch screens (one for Alice and one for Bob) are located at both ends of the case and display the GUI. The central component of the tangible interface is a manually shaped and soldered metal wire marble track. A 3D-printed marble dispenser at the beginning of the track (i.e., on Alice's side) integrates two buttons to capture Alice's value choice. Depending on which button is pressed, the dispenser releases the marble onto one of two subtracks, which then combine into a single main track. On this main track, the marble passes through three base gates: first Alice's, then Eve's, and finally Bob's. Each base gate has a rotary knob for configuring the base choice, an LED that visually indicates the current choice by color, and an inductive sensor that detects when a marble passes through it. The redirection mechanism located right after Bob's gate includes a solenoid that blocks one of the subtracks, effectively redirecting the marble. Laser-cut labels indicate which gate is for Alice, Bob, or Eve, as well as the two possible bases and measurement outcomes. Additionally, a 3D-printed container collects the marbles at the end of the track. Its key shape indicates that the photon values represented by the marbles form the final cryptographic key. A padlock-shaped laser-cut privacy shield can hide Eve.

Explanation Experience. User pairs first position themselves at the corresponding ends of *the Marb(e)lous BB84*. The privacy shield is placed on top of the tangible interface, covering Eve and preventing Alice and Bob from seeing each other's actions. From this moment, the GUI guides them through the explanation experience. After pressing "start" (see Figure 6, left), Marby first provides an introduction to the topic (i.e., explanation screens; see Figure 6, middle). It describes a secret message exchange scenario and proposes QKD as a method for securely exchanging a key to protect this message. It then briefly introduces BB84 (see AppendixE.2).

[5]The design of Marby is inspired by the marbles used in our TI and the atom-like symbol with multiple intercrossing orbits that frequently appears when searching for "Quantum" or "Quantum symbol" in image search engines such as Google Images, Yahoo Images, or freepik.com.

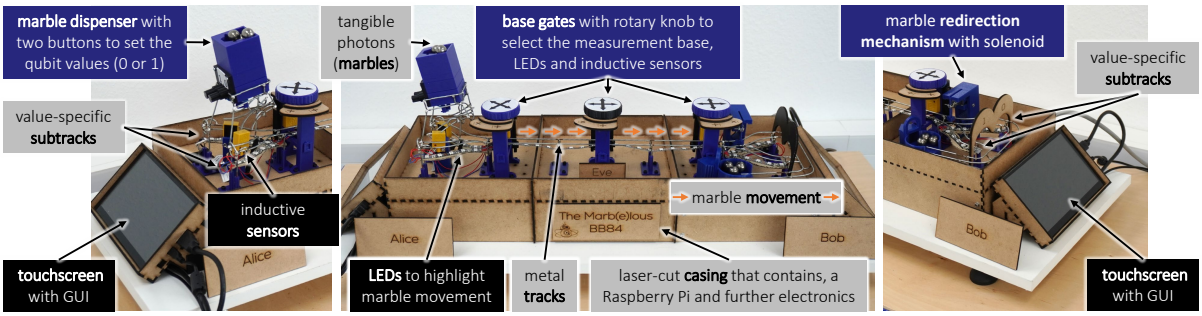


Fig. 7. In the final *the Marb(e)lous BB84*, marbles represent photons and travel from Alice (left) to Bob (right) along a metal track. Users select bases via rotary knobs, and LEDs indicate current configurations. A redirection mechanism maps measurement outcomes to value-specific subtracks. Two touch screens display a GUI that guides users through the protocol.

After this introduction, the protocol screen is displayed, which includes short textual instructions from Marby and a list of the currently exchanged values and bases. Alice and Bob are first instructed to configure their bases using their rotary knobs. The photon exchange starts with Alice choosing the first qubit's value by pressing one of two buttons on the marble dispenser. The released marble then passes through Alice's gate, the privacy shield, and Bob's gate. Based on the simulated measurement outcome at Bob's gate, the redirection mechanism directs the marble to the corresponding subtrack. Finally, the marble falls into the key-shaped container. The GUI then prompts further photon exchanges. After four repetitions, Alice can press a button to simulate the remaining photon exchanges. Next, users request their partner's bases via a button, which are visualized below their own choices. The following protocol steps are similary triggered through touch: (1) comparison of bases shown through colored boxes (see Figure 6, right), (2) reduction to measurements with matching bases only, (3) comparison of a subset of the remaining qubit values, which shows no differences as no eavesdropper is present, and (4) generation of the final key. All steps are only shown when the partner has reached the same screen.

Marby then explains that the security benefit of BB84 becomes clear when an eavesdropper, Eve, is introduced, and instructs users to remove the privacy shield so Eve becomes visible. Alice and Bob then perform the BB84 protocol again while collaboratively experimenting with different base configurations for Eve. However, they now observe differences between the two value subsets, and when proceeding to key generation, a message indicates that an eavesdropper was detected and that the key material is therefore insecure and cannot be used.

Answering RQ2 - Design

Designing a tangible interface to explain BB84 required *identifying recurring misunderstandings early on, which allowed us to prioritize meaningful interactions and explanatory clarity over formal completeness.* Our participatory and iterative design process improved the coherence of the resulting explanation, but also revealed a trade-off between design rigor and the substantial time and resources required to develop *the Marb(e)lous BB84*. Across the analyzed videos and workshop contributions, explanations commonly relied on *sequentially disclosing protocol elements and attack scenarios* to avoid overwhelming explainees. A *relatable motivational storyline grounded in everyday situations*, combined with *simple terminology* known from other contexts, may lower entry barriers for explainees and provide meaningful framing [9]. Collaborative and playful interactions were proposed to support engagement and motivation. Participants' designs further *materialized the otherwise imperceptible* through physical proxies and direct tangible interaction, which may support embodied cognition, information processing, and distributed cognition [9].

6 COMPARISON STUDY: EVALUATING THE MARB(E)LOUS BB84

We compared *the Marb(e)lous BB84* to a slide presentation and the most popular video in a user study ($N = 43$).

6.1 Method

6.1.1 Preparing the Comparison Baselines. We selected two baseline conditions: (1) the most popular video from our analysis and (2) a slide presentation, as the professionals' survey showed this was the most commonly used tool. We invited QKD researchers to provide used slides via an online survey that included informed consent, demographics, questions about their BB84 expertise, and the context of their slide use. One researcher (male, 32) provided a .pptx presentation, reporting high knowledge and prior use in teaching, external, and internal presentations. We anonymized the slides by removing logos and adjusting colors, then added introductory slides on the protocol's goal, polarization bases, and photon values, as well as a final slide illustrating Eve's impact.

6.1.2 Study Design. The independent variable of our comparison study was the *explanation method*, with three conditions: *tangible*, *video*, and *slides*. Given the limited motivation to learn about cybersecurity in the general public, unfounded (mis-)trust observed in users and frequent misunderstandings reported in related works [48, 79, 83, 88], we specifically set out to explore the different explanation methods' impact on the understanding and trust in the BB84 protocol, as well as their usability, and user experiences. We, therefore, employed a between-groups design to compare their effects on BB84 understanding among participants with little or no prior knowledge. This would not be possible if the same participants experienced all three different explanation methods. Moreover, repeated assessment across conditions would have required partitioning the BB84 protocol into subtopics of comparable complexity, administering separate pre- and post-tests for each, and – to control for order effects – developing equivalent explanations for each subtopic across all methods [8]. Beyond the considerable overhead, such a design would likely confuse participants, as it requires switching between methods within a single topic (i.e., the BB84 protocol), and reduce ecological validity, since explainees typically encounter explanations as uninterrupted narratives (see Section 4.2).

Instead, each of our between-groups conditions was conducted in a setting replicating typical real-world use. The *tangible* condition took place in the lab with pairs of participants. The *video* condition was conducted online and could be completed asynchronously within one week. The *slides* condition was conducted in two scheduled Zoom sessions with groups of 6 and 10 participants. Hence, while our between-groups design limits direct within-participant comparisons, it allows us to attribute observed effects to a single explanation method, as each participant is exposed to only one condition. All conditions lasted approximately 30 minutes.

Pre-Exposure Questionnaire. Participants completed an online survey covering demographics, affinity for technology (ATI) [39], security attitudes (SA-6) [37], and need for touch (NFT [75] with additional NFT+ items from [28]). Seven single-choice quiz questions about the BB84 protocol assessed participants' initial knowledge level (pre-test). Guided by [80], these quiz questions also included an "I don't know" option to discourage participants from guessing. Two attention checks ensured high data quality.

Exposure To Explanation. Participants then received the protocol explanation. The *tangible* group used *the Marb(e)lous BB84* together with a second participant. The *video* group watched the selected YouTube video at least once, with progression in the survey restricted until its duration elapsed. The *slides* group attended a live Zoom presentation delivered by an experimenter using the previously described slides. Participants were asked to turn on their cameras to ensure that they were actually present during the presentation.

Post-Exposure Questionnaire. After experiencing the explanation, participants completed the same BB84 quiz again (post-test), followed by assessments of usability (SUS [18]), workload (RTLX, aka. un-weighted NASA TLX [50]), user experience (UEQ-S) [63], and engagement (UES-SF [74]). We also applied the Interest/Enjoyment,

Table 2. An overview of the demographic information from participants of our comparison study, distinguished by group.

	Age					Gender			
	tangible	slides	video	overall		tangible	slides	video	overall
range	22 - 69	21 - 39	20 - 45	20 - 69	male	4	6	4	14
mean	31.23	26.44	29	28.72	female	8	10	10	28
std	12.21	4.29	8.54	8.70	other	1	0	0	1

Perceived Competence, and Value/Usefulness subscales of the Intrinsic Motivation Inventory (IMI [27, 70, 78]) and evaluated how the explanations might have impacted their trust in the BB84 protocol (HCTS [47]). Open-text questions captured the perceived benefits and challenges of each explanation method.

6.1.3 *Data Collection & Analysis.*

Quantitative Data. We calculated all standard scale scores as indicated in the corresponding original works (see Appendix C for details). To measure the effect of each method on participants' understanding of the BB84 protocol, we counted the number of correct answers each participant marked in the pre- and post-tests and calculated each participant's knowledge increase score. We analyzed all quantitative data descriptively and performed normality tests using the Shapiro-Wilk test and visual inspection of Q-Q plots. Next, we tested for significant differences among our three study groups using either a parametric one-way ANOVA (for standard distributions) or a nonparametric Kruskal–Wallis test (for non-normal distributions). We performed Holm's corrected Conover tests for post hoc comparisons when our initial tests indicated a significant difference.

Qualitative Data. We collected data through three free-text questions that asked participants to describe aspects of each method they liked and disliked, and to provide general feedback. One researcher grouped participants' short answers by themes (i.e., positive, negative, and improvement suggestions) and inductively derived corresponding codes.

6.1.4 *Recruitment.*

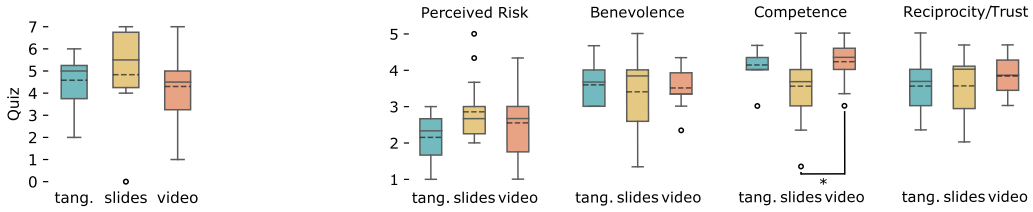
We recruited participants through institutional channels (social media and mailing lists). To avoid prior research, we did not mention QKD or BB84 in the invitation text, but described the study as explaining "a cybersecurity method." Participants could choose their study group to ensure informed consent, as conditions differed in required effort: the *video* condition was individual, the others included additional participants. Only the *tangible* condition required in-person attendance, and the *slides* condition required a microphone and webcam.

Participants signed up through an online survey, which also included five Likert items assessing prior cybersecurity expertise. One of these items asked if participants "know how QKD works and how it uses Quantum properties to exchange encryption keys securely." Only those not selecting "agree" or "strongly agree" qualified. The remaining items served to mask the study's focus on QKD and were not further analyzed. Participants in online conditions received 6€. Those who attended in person received 12€ to accommodate travel and waiting times. Each session lasted about 30 minutes.

6.1.5 *Limitations.*

We employed a between-groups design to measure the effect of each explanation method on understanding, but this approach limited direct comparisons between methods. In particular, we are unable to report on participants' comparative preferences. Participants were not randomly assigned to groups, as participation was in-person vs. online or required a webcam, which required an informed choice. This may have introduced sampling bias, limiting the internal validity of our findings [8]. To assess the impact on our findings, we analyzed between-groups differences in demographics, security attitudes, and need for touch in Section 6.2.1.

Moreover, we deliberately used different contextual settings for each condition to reflect how each explanation method is typically encountered in real-world usage (i.e., watching the YouTube video individually and asynchronously, joining a live online presentation as part of a larger audience, and using the TI in person together



(a) Understanding Increase

(b) HCTS Scores

Fig. 8. We measured the differences in participants' understanding of the BB84 protocol using pre- and post-quizzes. It increased across all conditions, with the largest gains for slides, followed by the tangible interface (see 8a). Trust ratings (HCTS) [47] show lower perceived risk and higher benevolence for the tangible interface, while video scored highest on competence and reciprocity (see 8b). Medians are solid, and means are dashed lines. * marks statistically significant differences.

with another user). This choice prioritizes ecological validity, but it also influences participants' experiences across conditions, thereby limiting the internal validity of our observations. Future work is needed to employ a more internal-validity–focused study design that better isolates the independent variable and evaluates the robustness of the effects we observed. Feedback on the TI may also reflect novelty bias, though we argue such first-time use mirrors real-world scenarios (see Section 4.1.1), reducing its impact on validity.

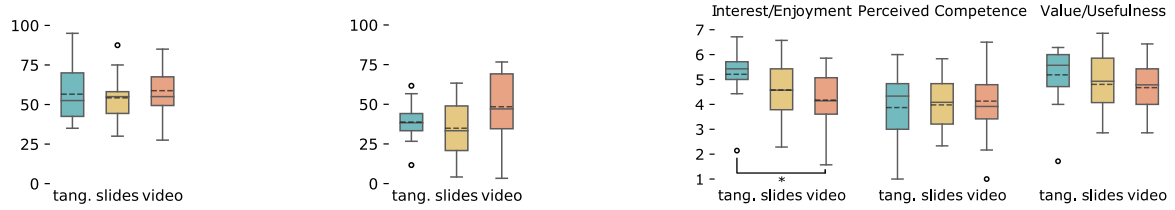
Our findings may further be affected by social desirability bias, and most participants were young females, limiting transferability to other demographics. Our group sample size aligns with related work, where user tests with $N = 12$ on educational interfaces identified over 98% of usability issues [6], but may still limit generalizability. Finally, given our exploratory focus, we compared specific instances of a *tangible*, *video*, and *slides*. Despite careful selection (see Section 6.1.1), future work is needed to confirm broader applicability and long-term effects.

6.2 Results

6.2.1 Participants. We recruited 43 participants for our comparison study: 13 in the *tangible* condition (one paired with an experimenter due to a last-minute cancellation), 16 in *slides*, and 14 in *video*. Four video participants failed one of two attention checks, but after manual review, we retained them, as no further signs of low effort were found in the data. No other participants failed attention checks. Participants were 20–69 years old ($mean = 28.72$, $std = 8.54$). 28 identified as female, 14 as male, and one as "other." Their average *affinity for technology interaction* was consistent with other university and social media–recruited samples [39] ($ATI = 4.00$, $std = 0.83$), but their overall *security attitudes score* ($SA{-}6 = 3.27$, $std = 0.62$) was below averages reported in [37], suggesting relatively low security interest. For the *extended need for touch (eNFT)*, we followed [28], assessing internal consistency of NFT and NFT+ items, which indicated acceptable reliability [85] (Cronbach's $\alpha = 0.95$). Participants' mean eNFT score was 4.24 ($std = 1.25$). Group comparisons revealed mean ages ranging from 26.44 to 32.23, with similar female-to-male ratios (Table 2). One-way ANOVAs comparing the different samples ATI, SA-6, and eNFT distributions found no significant differences ($F_{ATI} = 0.268$, $p_{ATI} = 0.766$; $F_{eNFT} = 2.541$, $p_{eNFT} = 0.091$; $F_{SA-6} = 0.304$, $p_{SA-6} = 0.740$), indicating that our subsamples are comparable.

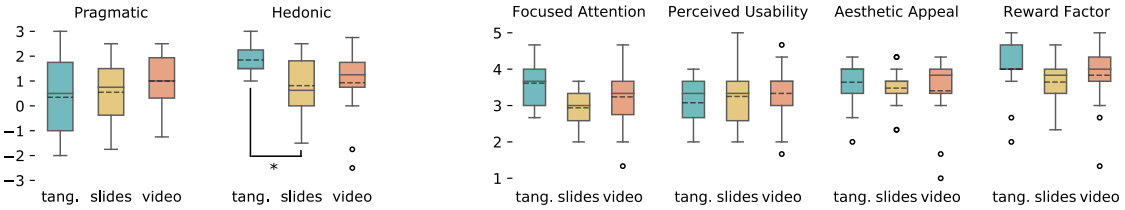
6.2.2 Quantitative Results. We only describe observed trends and statistically significant effects related to the *tangible* here. Appendix F.1 provides an overview of exact descriptive values and test results.

Understanding of & Trust in BB84. Participants' *understanding of the BB84 protocol increased* most for the *slides* group, followed by the *tangible* and *video* groups (see Figure 8a). We used the HCTS scale [47] to investigate the impact the *explanation methods* had on participants' trust in the BB84 protocol (see Figure 8b). The *perceived risk*



(a) SUS Scores (b) RTLX Scores (c) IMI Scores

Fig. 9. Participants rated the usability (SUS) and task load (RTLX) of the explanation methods. Medians are shown as solid lines and means as dashed lines. * marks statistically significant differences. SUS and RTLX ratings were comparable across conditions, with slightly higher workload for *video* (see 9a and 9b). We assessed participants' subjective experience with the different *explanation methods* through selected subscales of the intrinsic motivation inventory [78] (IMI). The *tangible* yielded the highest Interest/Enjoyment and Value/Usefulness, but lower Perceived Competence compared to *slides* and *video* (see 9c).



(a) User Experience as UEQ-S Scores (b) User Engagement as UES-SF Scores

Fig. 10. We applied the short versions of the User Experience Questionnaire (UEQ-S) [63] and the User Engagement Scale (UES-SF) [74] to assess user experience and engagement across the *explanation methods*. Medians are solid lines, means dashed lines, and * marks statistically significant differences. The *tangible* achieved higher hedonic quality and overall engagement, while *slides* and *video* scored higher on pragmatic quality and perceived usability.

was rated lowest for the *tangible* and its *benevolence* was rated highest. Nevertheless, in terms of *competence* and *reciprocity/trust*, the *video* condition received the highest ratings, followed by our *tangible* and *slides*.

System Usability & Task Load. All three explanation methods' *system usability* was rated as *"Ok"* [12], and the *task load* associated with interacting with them was *moderate* [46]. Both the *system usability* and the typically contrasting *task load* of the *video* were rated higher than those of our *tangible* (see Figures 9a and 9b).

Intrinsic Motivation Inventory (IMI). We used IMI subscales [78] to assess participants' subjective experiences when interacting with the different explanation methods (see Figure 9c). Participants rated their *interest and enjoyment* when using the *tangible* significantly higher compared to the *video* ($p = 0.0489$). Similarly, the *tangible's value and usefulness* was also rated highest, although not significantly. In contrast, participants *perceived their own competence* when interacting with the explanation methods lowest for the *tangible*.

User Experience (UEQ-S) & Engagement (UES-SF). The *overall user experience* of *the Marb(e)lous BB84* was rated *above average*, while *slides* and *video* were *below average* [52]. The UEQ-S distinguishes *pragmatic quality* (efficiency, perspicuity, and dependability) from *hedonic quality* (stimulation and novelty). The *hedonic quality* of our *tangible* in particular was rated significantly better compared to the *slides* ($p = 0.0471$). However, the *pragmatic quality* of *video* and *slides* was rated higher than the *tangible*. Similarly, participants rated the *tangible* highest in *aesthetic appeal*, *focused attention*, and *reward factor* on the UES-SF, but lowest in *perceived usability*.

6.2.3 Qualitative Results. Note that any comparisons described in the following reflect participants' unprompted, hypothetical opinions rather than actual experience, as they did not test multiple explanation methods.

Liked Aspects. Participants felt that the *tangible* and *video* explanations were *better than other methods*, mostly compared to text ($N_{tangible} = 4$, $N_{video} = 2$). Participants also appreciated that the explanations provided in the *slides* and *video* were *clear* ($N_{slides} = 3$, $N_{video} = 1$) and appreciated their example-based explanations ($N_{slides} = 1$, $N_{video} = 3$), as well as their visuals ($N_{video} = 3$, $N_{slides} = 2$). Moreover, the *simplicity of the provided explanation* was noted positively ($N_{slides} = 1$, $N_{video} = 2$) and participants felt *supported in their understanding* ($N_{slides} = 2$, $N_{video} = 1$). The *animations* used in both slides ($N_{slides} = 1$) and video ($N_{video} = 1$) were also well-received. Participants valued the option to *ask questions* in the *slides* ($N_{slides} = 2$) and the *video* was appreciated for its *stepwise explanation* ($N_{video} = 1$). Some participants of the *slides* and *tangible* group described the explanation as *fun and engaging* ($N_{slides} = 1$, $N_{tangible} = 1$). *The Marb(e)lous BB84* also received specific praise: the *physical representation* ($N_{tangible} = 3$), the *prototype itself* ($N_{tangible} = 2$), and the chance to *manipulate* it ($N_{tangible} = 3$) were assessed positively. Participants also felt like the *tangible interaction improved memory* ($N_{tangible} = 2$) and liked *experimenting by themselves* with the interface ($N_{tangible} = 2$).

Disliked Aspects & Suggestions for Improvement. Participants of all groups – but in particular from the slides group – wished for *more details on the protocol* ($N_{slides} = 5$, $N_{tangible} = 2$, $N_{video} = 1$). Participants also asked for *more background information* ($N_{slides} = 3$, $N_{tangible} = 3$). Especially the video groups often described the explanation pace as *too fast* ($N_{video} = 3$, $N_{slides} = 1$, $N_{tangible} = 1$). Slides were criticized for giving participants *no influence on pace* ($N_{slides} = 2$), and some noted *missing text* in slides ($N_{slides} = 1$) and video ($N_{video} = 2$). The explanations provided in these conditions were sometimes described as *too abstract* ($N_{slides} = 1$, $N_{video} = 1$) or having *too few illustrations* ($N_{video} = 2$). Some participants felt that other explanation methods might have been *better* ($N_{slides} = 1$, $N_{video} = 1$) and disliked the *speaker's voice pattern* ($N_{video} = 2$). In the tangible condition, several participants asked for *clearer task instructions* ($N_{tangible} = 3$). Participants also suggested *adding gamification features* ($N_{slides} = 1$, $N_{tangible} = 1$) to future experiences. Finally, the used terminology was sometimes described as *complicated* ($N_{video} = 1$, $N_{tangible} = 1$), and some did *not understand the protocol completely* ($N_{tangible} = 1$, $N_{slides} = 1$). Some participants also reported malfunctions of the *tangible* ($N_{tangible} = 2$) and *video* ($N_{video} = 1$).

Answering RQ3 - Comparison

By comparing *the Marb(e)lous BB84* to slides and a video, we identified *opportunities of using a tangible interface for cybersecurity explanations. The Marb(e)lous BB84* improved explainees' understanding similar to the baselines but was rated as slightly *more engaging, interesting, and enjoyable,* echoing findings from related work [65, 69]. High ratings in engagement and enjoyment are especially promising for cybersecurity, where motivation is critical. Professionals also expressed a preference for *hands-on experiments and simulations*, which tangible interfaces provide. Participants also valued the tangible interface's physical and interactive qualities, feeling that these enhanced memorability. This suggests that tangible cybersecurity explanation interfaces' primary advantage might lie in *enabling adult explainees to experience and experiment with normally abstract security concepts physically.* At the same time, several *challenges* emerged. The *quality of the cybersecurity explanation provided through a tangible to adults may be perceived as lacking* – as reflected in participants' low pragmatic quality, perceived usability, and perceived self-confidence ratings. Moreover, participants indicated that explainer support remained important, citing unclear instructions, occasional malfunctions, and difficulties with terminology – issues that also arose in other explanation methods.

Table 3. We used the listed Tangible Learning Design Guidelines by Antle and Wise [9] to reflect on the learning design of *the Marb(e)lous BB84*. As shown in the table, each guideline is based on a specific learning-theoretical perspective (first row).

Information Processing	**Constructivism**	**Embodied Cognition**	**Distributed Cognition**	**Computer-Supported Collaborative Learning**
G1: Distributing information across modalities can increase effective working memory capacity. **G2:** Making mappings between the form and behavior of physical and/or digital objects and real-world entities coherent can reduce extraneous cognitive load.	**G3:** Creating authentic tasks and using personal objects can help learners set individually meaningful goals for interacting with the tangible interface. **G4:** Using spatial, physical, temporal, or relational properties can slow down interaction and trigger reflection.	**G5:** Distributing parts of mental operations to actions on physical and/or digital objects can simplify and support mental skills. **G6:** Leveraging image schemas in input actions can improve usability and system learnability. **G7:** Using conceptual metaphor(s) grounded in image schemas to structure interaction mappings may bootstrap the learning of abstract concepts.	**G8:** Designing objects that allow spatial reconfiguration can enable mutual adaptation of ideas. **G9:** Using concrete representations can support the interpretation of symbolic representations of abstract concepts.	**G10:** Creating configurations in which participants can monitor each other's activity and gaze can support the development of shared understandings. **G11:** Distributing roles, information, and controls across the tangible interface learning environment can promote negotiation and collaboration. **G12:** Creating constrained or codependent access points schemes can compel learners to negotiate with each other.

7 DISCUSSION

As this work lies at the intersection of tangible learning and cybersecurity explanations, we use both the Tangible Learning Design Framework [9] and the Explainable Security paradigm [87] to derive *design implications for cybersecurity explanation (xSec) interfaces*. However, given our exploratory approach and small sample sizes, these implications should be interpreted as indicative rather than representative and require validation in future work.

7.1 Tangible Learning Design of The Marb(e)lous BB84

Grounded in the Tangible Learning Design Framework, we reflect on *the Marb(e)lous BB84* through *information processing*, *constructivism*, *embodied cognition*, *distributed cognition*, and *computer-supported collaborative learning* perspectives [9]. Table 3 lists all guidelines presented by Antle and Wise and their mapping to these theories. We structure this synthesis according to their taxonomy, distinguishing between *digital/physical objects*, *actions on objects*, *informational relations* (i.e., mapping of objects/actions to information), and the *learning activity*.

7.1.1 Digital/Physical Objects & Informational Relations. Quantum phenomena, data exchange, and security mechanisms are inherently invisible, making it challenging to establish coherent mappings between interface elements and their real-world counterparts, as suggested in G2. To address this, we used *tangible proxies* grounded in conceptual metaphors (G7): marbles and synchronized light animations represent photons, and rotating gates represent polarization filters. Such physical proxies *deliberately sacrifice realism to foreground only elements required for understanding*, reflecting explainers' and explainees' emphasis on conceptual clarity over detail and physical accuracy. They *leverage users' existing mental models through metaphors, but are consequently also limited by pre-existing knowledge*. For example, some users might conceptualize photons primarily as waves, which can make the marble metaphor confusing. We further presented information redundantly across multiple sensory modalities, as well as physical and digital modalities, using LEDs, separated tracks, and a GUI that displayed

chosen bases and values (G1, G9). Additional color-coded highlights reduced the mental operations required to compare outcomes (G5). At the same time, familiar interaction patterns (e.g., rotating a knob to select a basis) lowered entry barriers and exploited common sensorimotor schemas (G6).

xSec Interface Design Implication

We suggest using *tangible proxies* to potentially support embodied cognition and information processing [9], but paired with *narrative cues to correct potentially misleading metaphors.* While our findings showed similar learning gains for the different explanation methods, tangible interfaces can support the *distribution of mental tasks* across physical/digital objects, multiple sensory channels, and familiar actions [9], which is particularly important when explaining inherently abstract and invisible cybersecurity topics.

We did not explicitly consider image schemas[6] during our design process. Nevertheless, observations from our workshops – such as participants' suggestions to add privacy shields to represent boundaries in information access – indicate an *opportunity for future empirical research on intuitive mappings of image schemas to cybersecurity-related actions, such as exchanging information, limiting or granting access to data, protective measures, and common attacks.* Mehta et al.'s [71] work on preferred schemas for privacy control can guide this.

Finally, our design distributes roles and information across two explainees, encouraging coordination and mirroring the protocol's interdependence (G11). When the privacy shield is removed, users must additionally negotiate the configuration of Eve (G12) and can observe each other's actions (G10). However, we observed limited verbal coordination in our participants. We attribute this to the narrative around private and secret information, as some participants asked whether they were allowed to speak with each other as long as they kept their configurations secret.

xSec Interface Design Implication

Tangible multi-user interfaces are generally well-suited for collaborative learning [65]. However, *cybersecurity narratives emphasizing secrecy may suppress collaboration,* making explicit prompts and constrained cooperative tasks particularly important.

7.1.2 Actions on Objects. Findings from our comparison study further suggest that tangible interfaces (TIs) may support pauses and reflection, as both the video and the slide presentation were perceived as too quick. The sequencing of physical actions – choosing a basis, sending a marble, and observing its outcome – together with the GUI's stepwise explanation created a slowed interaction that encourages reflection (G4). Linear protocols or algorithms are particularly well-suited for such pacing, as their structure already consists of clearly delineated, dependent steps. Moreover, *the Marb(e)lous BB84* enables explainees to try different base-value combinations and observe their effects through immediate feedback. This aligns with professionals' survey responses, in which they envisioned explanation tools that support experimentation. While spatial reconfiguration as proposed in [9] is limited in *the Marb(e)lous BB84*, the action structure still makes the consequences of these changes clear (G8).

xSec Interface Design Implication

Based on our findings, we propose combining *self-paced temporal sequencing* with designs that enable explainees to *experiment with the consequences of their actions*, in order to externalize cybersecurity protocol logics and *allow pauses between actions*, thereby accommodating diverse stakeholder expertise and needs.

[6]Image schemas are abstract notions of recurring patterns of people's interactions that structure cognition [54]. They may describe spatial attributes, forces, processes, sensory attributes, identity, or relationships between entities.

7.1.3 Learning Activities. The learning activity itself – exchanging photons – would require minimal user interaction in real QKD systems. This is common across cybersecurity methods, where mechanisms are designed to be unobtrusive but still critical to understand [44, 76, 87]. Nevertheless, this mismatch between the learning task and real-world tasks can shift users' attention toward the interface rather than the explanation (G3). To mitigate this, we embedded the activity in a narrative, relatable storyline – exchanging a secret message – which most people have likely experienced before. We believe the similar understanding gains across all conditions in our comparison study reflect the usefulness of this framing. *However, future work is needed to establish a causal link between such narrative grounding and learning.*

xSec Interface Design Implication

Cybersecurity mechanisms are often designed to require minimal user interactions [44], making it *difficult to re-create authentic tasks during the learning experience.* We propose integrating *relatable storylines* as motivating contexts to address this challenge and ultimately support explainees' engagement and cognition [9].

7.2 Explainable Security Interfaces

We further discuss our findings through the lens of the Explainable Security (xSec) Paradigm [87], which provides a domain-specific framework for discussing the design implications of cybersecurity explanations targeting adults. xSec describes the "how" of cybersecurity explanations, the diverse stakeholders involved (who?), the content (what?), the reasons for explanations (why?), and their when and where.

7.2.1 Who Gives/Receives the Explanation? Where & When is the Explanation? Surveyed professionals reported explaining QKD in private, semi-public, and public environments. Across these contexts, explainers consistently assumed that explainees had limited prior knowledge. Correspondingly, both video analyses and workshop input emphasized starting with basic concepts – a need also supported by related work [11, 33, 81, 87]. Importantly, many of the explanation contexts we identified (e.g., exhibitions, private conversations, or early-stage decision-making) do not provide access to a running security system. Hence, while we acknowledge the importance of giving specific explanations of cybersecurity systems in situ as suggested in the xSec Paradigm [87], we argue that *decoupled cybersecurity explanation interfaces* – systems explicitly designed for explanation rather than embedded in security infrastructure – are particularly well-suited for broader adult cybersecurity explanations.

xSec Interface Design Implication

Our findings indicate that xSec interfaces should be *robust to highly diverse situational conditions* (e.g., presence of bystanders, limited time, noisy environments), while assuming *little prior expertise from explainees.* For explanations that are not tied to one specific system, this robustness may be best achieved through *decoupled xSec interfaces* [87].

7.2.2 What is Explained? While xSec describes security systems, security properties, threat models, vulnerabilities, and countermeasures as core content elements [87], our empirical results emphasize the importance of how and in which order these elements are introduced. Although the xSec paradigm does not explicitly list involved parties as required explanation content, our findings indicate that *presenting them early as human actors with relatable needs highlights real-world relevance and may help non-experts connect abstract mechanisms to meaningful use cases.* Workshop and survey participants noted that explainees often struggle to see the value of cybersecurity mechanisms, including QKD. *Real-world–inspired narratives (e.g., online shopping or government data protection), as observed in popular videos, may serve as an effective entry point to capture attention and motivate engagement.*

The remainder of our explanation addressed the security mechanism itself (i.e., BB84) and the threat model (i.e., Eve). *Our findings indicate that such an explanation should be presented step-wise to encourage pauses for reflection [9].* These steps may be derived from the inherent structure of the explained cybersecurity topic or by establishing a baseline of understanding before adding further information. In our prototype, we introduced the threat model (i.e., Eve) only after the core mechanism was understood.

Vigano and Magazzeni further describe that stakeholders require explanations at different levels of detail and with different aims [87]. However, implementing explanation interfaces that adapt content to individual needs, as explored in [82], remains challenging. *While large language models may enable new forms of personalization [30], future work is needed to investigate how personalization affects tangibility and collaborative learning dynamics.*

xSec Interface Design Implication

Based on our findings, we propose to introduce *human actors and real-world motivations before technical mechanisms.* Content should be *structured step-wise* [9]. Our observations suggest starting with core functionality and security goals, and only introducing threat models, vulnerabilities, and countermeasures once a baseline understanding is established.

7.2.3 Why Explainable Security? Vigano and Magazzeni argue that cybersecurity explanations are important because they increase confidence, trust, transparency, usability, adoption, accountability, verifiability, and testability [87]. In line with related work, our professionals' survey, workshops, and comparison study revealed misunderstandings and limited cybersecurity expertise among adult explainees [2, 26, 81, 88]. Prior work has therefore emphasized the importance of accessible and engaging formats for popular cybersecurity education, including comics, art, and film [21, 86, 97]. Our findings suggest that TIs could complement these approaches by enabling hands-on engagement with abstract security topics, *particularly in public or semi-public contexts such as exhibitions or outreach events.* In line with this, study participants suggested designing for playfulness, collaboration, exploration, and experimentation to increase motivation and sustain engagement in explainees. Prior work has also shown that TIs are particularly suited for hands-on, collaborative learning [10, 65, 69].

xSec Interface Design Implication

As misconceptions are prevalent and adult explainees' motivation to engage with cybersecurity might be limited [48, 88], xSec interfaces should *support informal, low-threshold engagement* through *playfulness, exploration, and collaboration* [30, 86, 87, 97]. We argue that tangible interfaces are particularly suitable to *complement existing popular security education approaches in (semi-)public settings*, as they enable collaborative, engaging, and curiosity-driven exploration of abstract security topics [30, 31, 65].

7.2.4 How to Explain Security? xSec describes that cybersecurity explanations can be provided in natural language, graphical languages (e.g., tree diagrams), formal languages (e.g., proofs and plans), or through gamification [87]. A connected recurring theme in our findings concerns the need to *balance accessibility and accuracy in cybersecurity explanations.* Our findings indicate that this could be achieved by using simple, yet accurate, terminology that may already be familiar to explainees from other contexts. In our interface, we therefore used the terms *bases* and *values* instead of *spins* and *polarizations* – a choice supported by workshop feedback, video analysis, and prior work [33, 35, 60]. This highlights that *terminology choices are not merely linguistic decisions, but shape perceived entry barriers.* Moreover, our findings highlighted the importance of identifying common misunderstandings early. *This observation underscores the necessity of involving both explainers and explainees participatorily in the design of cybersecurity explanation interfaces, as they can surface domain-specific and stakeholder-dependent misconceptions.*

xSec Interface Design Implication

xSec needs to *balance accessibility and accuracy* [87]. Our observations suggest that this could be achieved by carefully curating explanation content through *early-stage and iterative involvement of both explainers and explainees*. We propose to use terminology that reduces perceived complexity while maintaining correctness and to explicitly address common misconceptions in the explanation without delving into technical detail.

8 CONCLUSION

In this work, we explore cybersecurity explanations by designing *the Marb(e)lous BB84*, a tangible interface that explains the basic principles of the Quantum Key Distribution (QKD) protocol *BB84*. For this, we evaluated current QKD explanations through a survey ($N = 8$), conducted a thematic analysis of popular YouTube videos ($N = 10$), held a participatory workshop ($N = 9$) to derive design considerations, and implemented *the Marb(e)lous BB84*. In a comparison study ($N = 43$), we compared our interface with traditional QKD explanations in slides and videos between groups. The tangible received significantly higher ratings in hedonic quality than the slides and was rated more enjoyable than the video. We derive design implications for future cybersecurity explanation interfaces and contribute the first tangible interface for cybersecurity education targeting adult users.

Generative AI Usage Statement

We used Grammarly, DeepL Write, and ChatGPT 5.2 EDU to improve the text's language and phrasing and to check its grammar. We manually revised all changes suggested by these tools and take full responsibility for the content of this work. The rest of the content, including figures and tables, was created by us alone.

Acknowledgments

We would like to thank our study participants and the consulted QKD experts for their time and valuable input. This project has been funded by the European Union – NextGeneration EU and the dtec.bw – Center for Digitization and Technology Research of the Bundeswehr through the projects MuQuaNet and Voice of Wisdom.

References

[1] Ruba Abu-Salma, Elissa M. Redmiles, Blase Ur, and Miranda Wei. 2018. Exploring User Mental Models of End-to-End Encrypted Communication Tools. (Aug. 2018). https://www.usenix.org/conference/foci18/presentation/abu-salma

[2] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 137–153. doi:10.1109/SP.2017.65

[3] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (dec 1999), 40–46. doi:10.1145/322796.322806

[4] Omer Akgul, Wei Bai, Shruti Das, and Michelle L. Mazurek. 2021. Evaluating In-Workflow Messages for Improving Mental Models of End-to-End Encryption. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 447–464. https://www.usenix.org/conference/usenixsecurity21/presentation/akgul

[5] Mashari Alatawi and Nitesh Saxena. 2023. SoK: An Analysis of End-to-End Encryption and Authentication Ceremonies in Secure Messaging Systems. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Guildford United Kingdom, 187–201. doi:10.1145/3558482.3581773

[6] Roobaea Alroobaea and Pam J. Mayhew. 2014. How many participants are really enough for usability studies?. In *2014 Science and Information Conference*. 48–56. doi:10.1109/SAI.2014.6918171

[7] Kristina Andersen and Ron Wakkary. 2019. The Magic Machine Workshops: Making Personal Design Knowledge. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3290605.3300342

[8] Kylie Anglin, Qing Liu, and Vivian C Wong. 2024. A primer on the validity typology and threats to validity in education research. *Asia Pacific Education Review* 25, 3 (2024), 557–574. doi:10.1007/s12564-024-09955-4

[9] Alissa N. Antle and Alyssa F. Wise. 2013. Getting Down to Details: Using Theories of Cognition and Learning to Inform Tangible User Interface Design. *Interacting with Computers* 25, 1 (01 2013), 1–20. arXiv:https://academic.oup.com/iwc/article-pdf/25/1/1/2312459/iws007.pdf doi:10.1093/iwc/iws007

[10] Jatin Arora, Kartik Mathur, Manvi Goel, Piyush Kumar, Abhijeet Mishra, and Aman Parnami. 2020. Design and Evaluation of DIO Construction Toolkit for Co-making Shared Constructions. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 4, Article 127 (Sept. 2020), 25 pages. doi:10.1145/3369833

[11] Zahra Ashktorab, Justin D. Weisz, and Maryam Ashoori. 2019. Thinking Too Classically: Research Topics in Human-Quantum Computer Interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. doi:10.1145/3290605.3300486

[12] Aaron Bangor, Philip Kortum, and James Miller. 2009. Determining what individual SUS scores mean: adding an adjective rating scale. *J. Usability Studies* 4, 3 (May 2009), 114–123.

[13] Kristian Beckers and Sebastian Pape. 2016. A Serious Game for Eliciting Social Engineering Security Requirements. In *2016 IEEE 24th International Requirements Engineering Conference (RE)*. 16–25. doi:10.1109/RE.2016.39 ISSN: 2332-6441.

[14] Charles H Bennett. 1992. Quantum cryptography using any two nonorthogonal states. *Physical review letters* 68, 21 (1992), 3121.

[15] Charles H. Bennett and Gilles Brassard. 2014. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 560 (2014), 7–11. doi:10.1016/j.tcs.2014.05.025 Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[16] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. arXiv:https://doi.org/10.1191/1478088706qp063oa doi:10.1191/1478088706qp063oa

[17] V Braun and V Clarke. 2013. Successful thematic analysis.

[18] John Brooke. 1996. *SUS – a quick and dirty usability scale.* Taylor & Francis, 189–194.

[19] Ankur Chattopadhyay, Mohammad Q. Azhar, Thomas Everson, and Robert Ruska Jr. 2020. Integrated Cybersecurity Plus Robotics Lesson Using NAO. In *Proceedings of the 21st Annual Conference on Information Technology Education (SIGITE '20)*. Association for Computing Machinery, New York, NY, USA, 397–402. doi:10.1145/3368308.3415418

[20] Yan-Ming Chiou, Tia Barnes, Shameeka M Jelenewicz, Chrystalla Mouza, and Chien-Chung Shen. 2021. Teacher Views on Storytelling-based Cybersecurity Education with Social Robots. In *Proceedings of the 20th Annual ACM Interaction Design and Children Conference (IDC '21)*. Association for Computing Machinery, New York, NY, USA, 508–512. doi:10.1145/3459990.3465199

[21] Yan-Ming Chiou, Tia Barnes, Chrystalla Mouza, and Chien-Chung Shen. 2020. Social robot teaches cybersecurity. In *Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts (IDC '20)*. Association for Computing Machinery, New York, NY, USA, 199–204. doi:10.1145/3397617.3397824

[22] Design Council. [n. d.]. Framework for Innovation. https://www.designcouncil.org.uk/our-resources/framework-for-innovation/ last accessed on July 16, 2025.

[23] Rachel Cummings, Gabriel Kaptchuk, and Elissa M. Redmiles. 2021. "I need a better description": An Investigation Into User Expectations For Differential Privacy. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Virtual Event Republic of Korea, 3037–3052. doi:10.1145/3460120.3485252

[24] Clifford De Raffaele, Serengul Smith, and Orhan Gemikonakli. 2018. An Active Tangible User Interface Framework for Teaching and Learning Artificial Intelligence. In *Proceedings of the 23rd International Conference on Intelligent User Interfaces* (Tokyo, Japan) *(IUI '18)*. Association for Computing Machinery, New York, NY, USA, 535–546. doi:10.1145/3172944.3172976

[25] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. 2019. In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, Stockholm, Sweden, 401–415. doi:10.1109/EuroSP.2019.00037

[26] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. 2019. In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. 401–415. doi:10.1109/EuroSP.2019.00037

[27] Edward L. Deci, Haleh Eghrari, Brian C. Patrick, and Dean R. Leone. 1994. Facilitating Internalization: The Self-Determination Theory Perspective. *Journal of Personality* 62, 1 (1994), 119–142. arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1467-6494.1994.tb00797.x doi:10.1111/j.1467-6494.1994.tb00797.x

[28] Sarah Delgado Rodriguez, Priyasha Chatterjee, Anh Dao Phuong, Florian Alt, and Karola Marky. 2024. Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 981, 23 pages. doi:10.1145/3613904.3642863

[29] Sarah Delgado Rodriguez, Anh Dao Phuong, Franziska Bumiller, Lukas Mecke, Felix Dietz, Florian Alt, and Mariam Hassib. 2023. Padlock, the Universal Security Symbol? - Exploring Symbols and Metaphors for Privacy and Security. In *Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia*. ACM, Vienna Austria, 10–24. doi:10.1145/3626705.3627770

[30] Sarah Delgado Rodriguez, Sarah Elisabeth Winterberg, Franziska Bumiller, Felix Dietz, Florian Alt, and Mariam Hassib. 2025. XSec Companions: Exploring the Design of Cybersecurity Companions. In *2025 European Symposium on Usable Security (EuroUSEC)*. 204–220. doi:10.1109/EuroUSEC69254.2025.00028

[31] Sarah Delgado Rodriguez, Maximiliane Windl, Florian Alt, and Karola Marky. 2025. The TaPSI Research Framework - A Systematization of Knowledge on Tangible Privacy and Security Interfaces. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 923, 28 pages. doi:10.1145/3706598.3713968

[32] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. 2013. Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13)*. Association for Computing Machinery, New York, NY, USA, 915–928. doi:10.1145/2508859.2516753

[33] Seth DeVore and Chandralekha Singh. 2020. Interactive learning tutorial on quantum key distribution. *Phys. Rev. Phys. Educ. Res.* 16 (May 2020), 010126. Issue 1. doi:10.1103/PhysRevPhysEducRes.16.010126

[34] Whitfield Diffie and Martin E. Hellman. 2022. New Directions in Cryptography. (2022), 365–390. https://doi.org/10.1145/3549993.3550007

[35] W. Dür and S. Heusler. 2013. What we can learn about quantum physics from a single qubit. doi:10.48550/ARXIV.1312.1463

[36] Wolfgang Dür and Stefan Heusler. 2016. The Qubit as Key to Quantum Physics Part II: Physical Realizations and Applications. *The Physics Teacher* 54, 3 (March 2016), 156–159. doi:10.1119/1.4942137

[37] Cori Faklaris, Laura Dabbish, and Jason Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Berkeley, CA, Santa Clara, CA, USA. doi:10.13140/RG.2.2.29840.05125/3

[38] M. Fjeld, D. Hobi, L. Winterthaler, B. Voegtli, and P. Juchli. 2004. Teaching electronegativity and dipole moment in a TUI. In *IEEE International Conference on Advanced Learning Technologies, 2004. Proceedings.* 792–794. doi:10.1109/ICALT.2004.1357659

[39] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467.

[40] José A. Gallud, Ricardo Tesoriero, Maria D. Lozano, Victor M. R. Penichet, and Habib M. Fardoun. 2022. The Use of Tangible User Interfaces in K12 Education Settings: A Systematic Mapping Study. *IEEE Access* 10 (2022), 24824–24842. doi:10.1109/ACCESS.2022.3154794

[41] Alexandre Gillet, Michel Sanner, Daniel Stoffler, and Arthur Olson. 2005. Tangible interfaces for structural molecular biology. *Structure* 13, 3 (2005), 483–491.

[42] Mark Gondree and Zachary N. J. Peterson. 2013. Valuing Security by Getting [d0x3d!]: Experiences with a Network Security Board Game. https://www.usenix.org/conference/cset13/workshop-program/presentation/gondree

[43] Robert Goodfellow. 2016. Quantum Key Distribution: Leveraging the Laws of Physics for Perfectly Secure One-Time Pad Encryption. (2016).

[44] Peter Leo Gorski, Luigi Lo Iacono, and Matthew Smith. 2023. Eight Lightweight Usable Security Principles for Developers. *IEEE Security & Privacy* 21, 1 (2023), 20–26. doi:10.1109/MSEC.2022.3205484

[45] Ingrid Graffer, Maria B Line, and Karin Bernsmed. 2015. Play2Prepare: A Board Game Supporting IT Security Preparedness Exercises for Industrial Control Organizations. (2015).

[46] Rebecca Grier. 2015. How high is high? A metanalysis of NASA TLX global workload scores. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 59. doi:10.1177/1541931215591373

[47] Siddharth Gulati, Sonia Sousa, and David Lamas. 2019. Design, development and evaluation of a human-computer trust scale, journal = Behaviour & Information Technology. 38, 10 (2019), 1004–1015. doi:10.1080/0144929X.2019.1656779

[48] Julie M. Haney and Wayne G. Lutters. 2018. "It's Scary…It's Confusing…It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 411–425. https://www.usenix.org/conference/soups2018/presentation/haney-perceptions

[49] Stephen Hart, Andrea Margheri, Federica Paci, and Vladimiro Sassone. 2020. Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security* 95 (Aug. 2020), 101827. doi:10.1016/j.cose.2020.101827

[50] Sandra G. Hart and Lowell E. Staveland. 1988. Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. In *Human Mental Workload*, Peter A. Hancock and Najmedin Meshkati (Eds.). Advances in Psychology, Vol. 52. North-Holland, 139–183. doi:10.1016/S0166-4115(08)62386-9

[51] Stefan Heusler and Malte Ubben. 2019. A Haptic Model of Entanglement, Gauge Symmetries and Minimal Interaction Based on Knot Theory. *Symmetry* 11, 11 (2019). doi:10.3390/sym11111399

[52] Andreas Hinderks, Martin Schrepp, and Jörg Thomaschewski. 2018. A benchmark for the short version of the user experience questionnaire. In *Proceedings of the 14th International Conference on Web Information Systems and Technologies-APMDWE*. SciTePress, 373–377.

[53] Deborah Hix and HR Hartson. 1992. Formative Evaluation: Ensuring Usability in User Interfaces.

[54] Jörn Hurtienne and Johann Habakuk Israel. 2007. Image schemas and their metaphorical extensions: intuitive patterns for tangible interaction. In *Proceedings of the 1st International Conference on Tangible and Embedded Interaction* (Baton Rouge, Louisiana) *(TEI '07)*. Association for Computing Machinery, New York, NY, USA, 127–134. doi:10.1145/1226969.1226996

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

[56] Klementyna Jankiewicz, Piotr Migdal, and Pawel Grabarz. 2022. Virtual Lab by Quantum Flytrap: Interactive Simulation of Quantum Mechanics. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts* (New Orleans, LA, USA) *(CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, Article 175, 4 pages. doi:10.1145/3491101.3519885

[57] Farzaneh Karegar, Ala Sarah Alaqra, and Simone Fischer-Hübner. 2022. Exploring {User-Suitable} metaphors for differentially private data analyses. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 175–193.

[58] M. Fahim Ferdous Khan, Damar Masato Hadisumarto, and Ken Sakamura. 2022. A Tangible-Tool-Based Lesson Plan on Cipher Key Exchange Protocol for Early-Stage Learners. In *2022 IEEE Global Engineering Education Conference (EDUCON)*. 620–627. doi:10.1109/EDUCON52537.2022.9766379

[59] Hyeok Kim, Mingyoung Jessica Jeng, and Kaitlin N Smith. 2025. Toward Human-Quantum Computer Interaction: Interface Techniques for Usable Quantum Computing. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, 1–18. doi:10.1145/3706598.3713370

[60] Antje Kohnle and Aluna Rizzoli. 2017. Interactive simulations for quantum key distribution. *European Journal of Physics* 38, 3 (mar 2017), 035403. doi:10.1088/1361-6404/aa62c8

[61] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. 2017. "I Have No Idea What I'm Doing" - On the Usability of Deploying HTTPS. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 1339–1356. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/krombholz

[62] Victoria Kunde, Jan Magnus Nold, and Jonas Hielscher. 2024. "Everything We Encrypt Today Could Be Cracked" — Exploring (Post) Quantum Cryptography Misconceptions. In *Proceedings of the 2024 European Symposium on Usable Security (EuroUSEC '24)*. Association for Computing Machinery, New York, NY, USA, 125–136. doi:10.1145/3688459.3688468

[63] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and evaluation of a user experience questionnaire. In *Symposium of the Austrian HCI and usability engineering group*. Springer, 63–76.

[64] James R. Lewis. 1994. Sample Sizes for Usability Studies: Additional Considerations. *Human Factors* 36, 2 (1994), 368–378. arXiv:https://doi.org/10.1177/001872089403600215 doi:10.1177/001872089403600215 PMID: 8070799.

[65] Yanhong Li, Meng Liang, Julian Preissing, Nadine Bachl, Michelle Melina Dutoit, Thomas Weber, Sven Mayer, and Heinrich Hussmann. 2022. A Meta-Analysis of Tangible Learning Studies from the TEI Conference. In *Sixteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Daejeon, Republic of Korea) *(TEI '22)*. Association for Computing Machinery, New York, NY, USA, Article 7, 17 pages. doi:10.1145/3490149.3501313

[66] Andrea López-Incera and Wolfgang Dür. 2019. Entangle me! A game to demonstrate the principles of quantum mechanics. *American Journal of Physics* 87, 2 (2019), 95–101.

[67] Ákos Lédeczi, MiklÓs MarÓti, Hamid Zare, Bernard Yett, Nicole Hutchins, Brian Broll, Péter Völgyesi, Michael B. Smith, Timothy Darrah, Mary Metelko, Xenofon Koutsoukos, and Gautam Biswas. 2019. Teaching Cybersecurity with Networked Robots. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19)*. Association for Computing Machinery, New York, NY, USA, 885–891. doi:10.1145/3287324.3287450

[68] Panos Markopoulos and Mathilde Bekker. 2003. Interaction design and children. 141-149 pages. arXiv:https://academic.oup.com/iwc/article-pdf/15/2/141/7800146/iwc15-0141.pdf doi:10.1016/S0953-5438(03)00004-3

[69] Paul Marshall. 2007. Do tangible interfaces enhance learning?. In *Proceedings of the 1st International Conference on Tangible and Embedded Interaction* (Baton Rouge, Louisiana) *(TEI '07)*. Association for Computing Machinery, New York, NY, USA, 163–170. doi:10.1145/1226969.1227004

[70] Edward McAuley, Terry Duncan, and Vance V Tammen. 1989. Psychometric properties of the Intrinsic Motivation Inventory in a competitive sport setting: A confirmatory factor analysis. *Research quarterly for exercise and sport* 60, 1 (1989), 48–58.

[71] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, Bashar Nuseibeh, and Daniel Gooch. 2021. Up Close & Personal: Exploring User-Preferred Image Schemas for Intuitive Privacy Awareness and Control. In *Proceedings of the Fifteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Salzburg, Austria) *(TEI '21)*. Association for Computing Machinery, New York, NY, USA, Article 7, 13 pages. doi:10.1145/3430524.3440626

[72] Jason Mickelson and Wendy Ju. 2010. Math propulsion: engaging math learners through embodied performance & visualization. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction* (Funchal, Portugal) *(TEI '11)*. Association for Computing Machinery, New York, NY, USA, 101–108. doi:10.1145/1935701.1935722

[73] Alan Mills, Jonathan White, and Phil Legg. 2024. Cyber Funfair: Creating Immersive and Educational Experiences for Teaching Cyber Physical Systems Security. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1* (Portland, OR, USA) *(SIGCSE 2024)*. Association for Computing Machinery, New York, NY, USA, 847–852. doi:10.1145/3626252.3630820

[74] Heather L O'Brien, Paul Cairns, and Mark Hall. 2018. A practical approach to measuring user engagement with the refined user engagement scale (UES) and new UES short form. *International Journal of Human-Computer Studies* 112 (2018), 28–39.

[75] Joann Peck and Terry L. Childers. 2003. Individual Differences in Haptic Information Processing: The "Need for Touch" Scale. *Journal of Consumer Research* 30, 3 (12 2003), 430–442. arXiv:https://academic.oup.com/jcr/article-pdf/30/3/430/11425838/30-3-430.pdf doi:10.1086/378619

[76] Davy Preuveneers, Wouter Joosen, Mustafa A Mustafa, Aysajan Abidin, and Enrique Argones Rúa. [n. d.]. Frictionless authentication systems: Emerging trends, research challenges and opportunities. In *the 11th Int. Conf. on Emerging Security Information, Systems and Technologies, SECURWARE*, Vol. 17.

[77] Adrian Reuter, Ahmed Abdelmaksoud, Karima Boudaoud, and Marco Winckler. 2021. Usability of End-to-End Encryption in E-Mail Communication. *Frontiers in Big Data* 4 (July 2021). doi:10.3389/fdata.2021.568284 Publisher: Frontiers.

[78] Richard M Ryan, Valerie Mims, and Richard Koestner. 1983. Relation of reward contingency and interpersonal context to intrinsic motivation: A review and test using cognitive evaluation theory. *Journal of personality and Social Psychology* 45, 4 (1983), 736. https://psycnet.apa.org/doi/10.1037/0022-3514.45.4.736

[79] John Sadik and Scott Ruoti. 2025. A Large-Scale Survey of Password Entry Practices on Non-Desktop Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 9, 3, Article 125 (Sept. 2025), 30 pages. doi:10.1145/3749491

[80] Thomas Samuel, Razia Azen, and Naira Campbell-Kyureghyan. 2019. Evaluation of Learning Outcomes through Multiple Choice Pre-and Post-Training Assessments. *Journal of Education and Learning* 8, 3 (2019), 122–135.

[81] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2022. Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours. In *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers* (Copenhagen, Denmark). Springer-Verlag, Berlin, Heidelberg, 248–265. doi:10.1007/978-3-031-25460-4_14

[82] Lorin Schöni, Neele Roch, Hannah Sievers, Martin Strohmeier, Peter Mayer, and Verena Zimmermann. 2025. It's a Match - Enhancing the Fit between Users and Phishing Training through Personalisation. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 592, 25 pages. doi:10.1145/3706598.3713845

[83] Svenja Schroeder, Markus Huber, David Wind, and Christoph Rottermanner. 2016. When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging. In *Proceedings 1st European Workshop on Usable Security*. Internet Society, Darmstadt, Germany. doi:10.14722/eurousec.2016.23012

[84] Elias Shamilov, Nirit Gavish, Hagit Krisher, and Eran Horesh. 2018. Tangible User Interface. In *Engineering Psychology and Cognitive Ergonomics: 15th International Conference, EPCE 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, July 15-20, 2018, Proceedings* (Las Vegas, NV, USA). Springer-Verlag, Berlin, Heidelberg, 471–479. doi:10.1007/978-3-319-91122-9_38

[85] Keith S Taber. 2018. The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education* 48, 6 (2018), 1273–1296.

[86] Luca Viganò. 2022. Don't Tell Me the Cybersecurity Moon Is Shining.... In *Imagine Math 8: Dreaming Venice*, Michele Emmer and Marco Abate (Eds.). Springer International Publishing, Cham, 455–477. doi:10.1007/978-3-030-92690-8_30

[87] Luca Viganò and Daniele Magazzeni. 2020. Explainable Security. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 293–300. doi:10.1109/EuroSPW51379.2020.00045

[88] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) *(SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, Article 11, 16 pages. doi:10.1145/1837110.1837125

[89] Jonathan White, Phil Legg, and Alan Mills. 2023. Interactive cyber-physical system hacking: Engaging students early using scalextric. *Journal of The Colloquium for Information Systems Security Education* 10, 6. Issue 1. doi:10.53735/cisse.v10i1.163 Conference paper was uploaded within 3 months of acceptance. Date of acceptance remains the same for the journal article..

[90] Alma Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *8th USENIX Security Symposium (USENIX Security 99)*. USENIX Association, Washington, D.C. https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50

[91] Margaret Wilson. 2002. Six views of embodied cognition. *Psychonomic Bulletin & Review* 9, 4 (December 2002), 625—636. doi:10.3758/bf03196322

[92] Aiping Xiong, Tianhao Wang, Ninghui Li, and Somesh Jha. 2020. Towards Effective Differential Privacy Communication for Users' Data Sharing Decision and Comprehension. doi:10.48550/arXiv.2003.13922 arXiv:2003.13922 [cs].

[93] Affan Yasin, Lin Liu, Tong Li, Rubia Fatima, and Wang Jianmin. 2019. Improving software security awareness using a serious game. *IET Software* 13, 2 (April 2019), 159–169. doi:10.1049/iet-sen.2018.5095

[94] Bernard Yett, Nicole Hutchins, Gordon Stein, Hamid Zare, Caitlin Snyder, Gautam Biswas, Mary Metelko, and Ákos Lédeczi. 2020. A Hands-On Cybersecurity Curriculum Using a Robotics Platform. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*. Association for Computing Machinery, New York, NY, USA, 1040–1046. doi:10.1145/3328778.3366878

[95] Alexander Zable, Lloyd Hollenberg, Eduardo Velloso, and Jorge Goncalves. 2020. Investigating Immersive Virtual Reality as an Educational Tool for Quantum Computing. In *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology (VRST '20)*. Association for Computing Machinery, New York, NY, USA, 1–11. doi:10.1145/3385956.3418957

[96] Arooj Zaidi, Giulia Barbareschi, Kai Kunze, Yun Suen Pai, and Junichi Yamaoka. 2025. TIEboard: A Digital Educational Tool for Kids Geometric Learning. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 9, 2, Article 62 (June 2025), 27 pages. doi:10.1145/3729478

[97] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2016. The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity. *International Journal of Human–Computer Interaction* 32, 3 (2016), 215–257. arXiv:https://doi.org/10.1080/10447318.2016.1136177 doi:10.1080/10447318.2016.1136177

A QKD PROFESSIONALS SURVEY

A.1 Scenario Descriptions

We asked QKD professionals to rate their experiences with the following scenarios: (1) A *marketing scenario* where you explain something to someone about QKD to sell a product or idea. (2) An *external presentation scenario* where you have explained something about QKD to someone, to present your company/project externally (e.g., to external visitors or trade fairs). (3) An internal scenario where you have explained something about QKD to someone who is part of your 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 in which you explained something about QKD to acquaintances, friends, or relatives (e.g., to tell them about their job)

A.2 Professionals' Expertise and Experiences

Table 4. We asked QKD professionals ($N = 8$) to rate their expertise with QKD, how they perceived explaining QKD, and how often they might have experienced different explanation scenarios. All Likert items used a 5-point scale from 1 (disagree) to 5 (agree).

item	median
understand physical effects	4.50
understand QKD protocols	5.00
develop QKD hardware	1.00
develop QKD software	1.00
use QKD hardware	2.00
use QKD simulation software	1.50
use software to control QKD hardware	3.00

(a) QKD Expertise

item	median
topic easy to explain	4.00
topic easy to understand	2.00
explanations easy to understand	4.00
got positive feedback	4.00
use tools from others	3.50
use own tools	4.00
no further tools needed	3.00

(b) Explanation Experiences

	0	1-5	6-15	>15
Marketing	3	3	0	2
External	2	3	0	3
Internal	0	3	2	3
Exhibition	6	0	2	0
Teaching	4	2	1	1
Private	0	3	4	1

(c) Scenario Frequencies

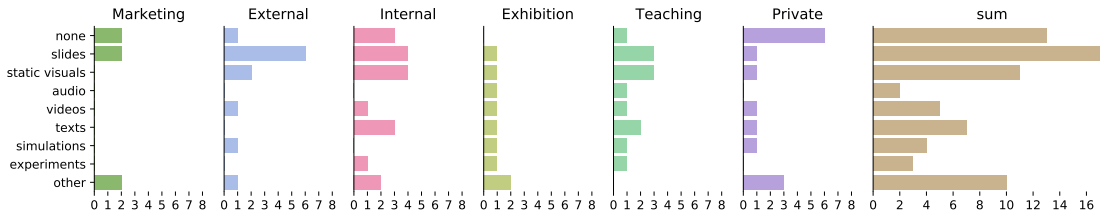


Fig. 11. Materials and tools our participants have used in diverse scenarios in the past.

A.3 Professionals' Perceptions of Explainees per Scenario

Table 5. Explainee's motivation to understand QKD (M) and QKD expertise (E) as indicated by our participants on a scale ranging from 1 to 5. "Exp." refers to participants who have experienced this scenario, and "hypo." lists the other participants' ratings.

	Marketing				**External**				**Internal**		**Exhibition**				**Teaching**				**Private**	
	exp.		**hypo.**		**exp.**		**hypo.**		**exp.**		**exp.**		**hypo.**		**exp.**		**hypo.**		**exp.**	
	M	**E**	**M**	**E**	**M**	**E**	**M**	**E**	**M**	**E**	**M**	**E**	**M**	**E**	**M**	**E**	**M**	**E**	**M**	**E**
mean	3.75	2.75	2.20	1.60	3.33	3.17	3.50	2.0	3.79	2.86	3.25	2.00	3.71	1.43	3.83	2.83	3.50	2.17	2.67	1.42
std	1.89	1.71	0.84	0.89	1.44	1.11	0.71	0.0	1.25	1.56	0.50	0.82	1.38	1.13	0.75	1.60	0.55	0.75	1.07	0.51
mdn	4.50	2.50	2.00	1.00	4.00	3.00	3.50	2.0	4.00	3.00	3.00	2.00	4.00	1.00	4.00	3.00	3.50	2.00	3.00	1.00

B YOUTUBE VIDEO ANALYSIS: CODEBOOK

Table 6. Codebook of YouTube Video Analysis.

Motivating Scenarios	
code	count
online retail	2
messaging	2
government secrets	1
protect information	4

Additional Topics	
code	count
security through computing effort	3
Encryption	2
Q-Day	4
Public Key Cryptography	3
E91	1
Cyphertext	2
Shift cipher	1

Quantum Theory	
Heisenberg uncertainty	2
No cloning theorem	3
Superposition	3
Entanglement	3

Protocol Elements	
code	count
Base selection is random	8
Base exchange	6
Delete unmatching bases	8
Eve influences states	9
Eavesdropper detection	8
Key Generation	9
Message uses public channel	6

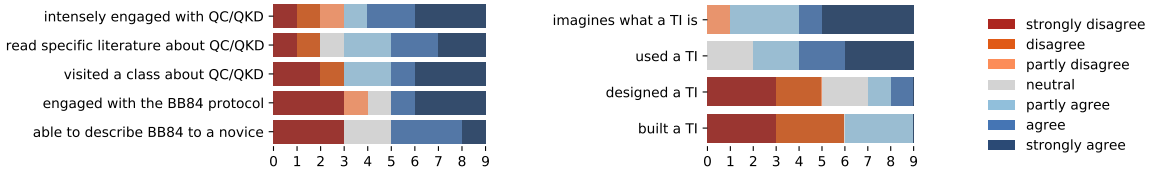
Terminology	
code	count
Alice	10
Bob	10
Eve	4
photon	5
qubit	2
base	5
filter	2
measurement	1
Scheme diagonal	4
Scheme rectilininear	3
photon polarization	6
bit values	8
spin	1

C CALCULATION OF STANDARD SCALE SCORES

We reverse-coded the values of negatively worded items and calculated the means for the ATI [39], SA-6 [37], extended NFT (eNFT) [28], UEQ-S subscales [63] (we here first subtracted 4 to transform the scale to -3 - +3 range), UES-SF subscales [74], IMI subscales [27, 78], and HCTS subscales [47]. For calculating SUS scores, we first subtracted 1 to transform values to a 0-4 range, then summarized all values per participant, and finally multiplied them by 2.5 [18]. RTLX scores were calculated by translating values to a 0 to 20 range (i.e., by subtracting 1), multiplying them by 5, and then calculating their mean [46, 50].

D PARTICIPATORY WORKSHOPS

D.1 Participants' Previous Expertise and Experiences



(a) QKD and Quantum Computing (QC) Expertise (b) Experience with Tangible Interfaces (TIs)

Fig. 12. We captured our workshop participants' ($N = 9$) previous experiences with Quantum Computing and tangible interfaces through a questionnaire with 7-point Likert Scales.

D.2 Descriptions of Magic Machines

We describe our participants' design ideas for TIs that explain the BB84 protocol below. For clarity, we assigned a name to each prototype.

Air Hockey (Group 1, students). Group 1 proposed a table-like, two-user interface with a central screen that served as a privacy screen and displayed instructions to both users. Photons were represented by rectangular chips. Alice selected the value by turning the chip around before passing it through a base gate. Bob then measured it by passing it through one of his gates. The system revealed matching bases and the resulting key, while Eve could be introduced by placing a physical object next to the screen, triggering simulated interference.

Puzzle Box (Group 2, students). Group 2 designed a box-shaped interface that emphasized how measurement irreversibly changes a photon's state rather than explaining the full BB84 protocol. Alice and Bob are positioned on opposite sides. They pressed malleable, plasticine-like photons through differently shaped base holes, with mismatches permanently altering the photon.

Geometric Blocks (Group 3, students). Group 3 envisioned a table-like, two-user interface with a central privacy screen and integrated displays. The interface could also be used alone, by folding the screen away. Bases were represented by geometric objects placed. Two positions shown on Alice's bottom screen represented values and triggered photon transmission. Bob then received a signal (sound or light) and placed a base on his side to trigger the measurement. Eve was envisioned as system-simulated or as a third participant.

QKD Call (Group 4, curators). The curators sketched a stand-alone interface operated by a single explainee in Bob's role. Alice guided the explanation remotely via voice or video call, while Bob selected bases using a rotary wheel. The screen displayed exchanged bases and measured values. Bob selects matching bases with buttons. In the final step, the interface visualizes discrepancies between a subset of their values and prompts Bob to decide whether Eve was present.

E DEVELOPMENT OF THE MARB(E)LOUS BB84

E.1 3D Model of First Vision

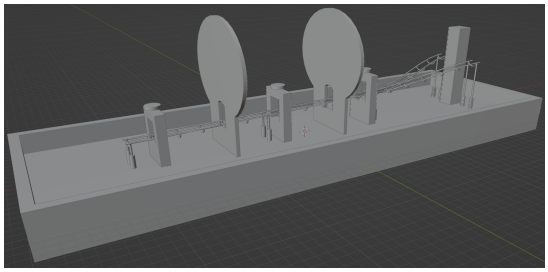


Fig. 13. Screenshot of a 3D model showing the envisioned design of *the Marb(e)lous BB84*. We used this model to explain our concept to two QKD researchers and gather early feedback before implementing the prototype.

E.2 Explanation Script Delivered in the Final GUI

E.2.1 Introduction Screens Textcontents (Alice Version). Hi Alice! It's nice to meet you! I'm Marby, I can explain how Quantum Key Distribution works!
So you want to send a secret message to Bob? You can encrypt it using a secret key you both know. When Bob receives it, he can use the same key to decrypt it, but nobody else can read it without the key!
To make sure that only you and Bob know the right key, it must be first exchanged securely. Quantum Key Distribution (QKD) is a great method to exchange such keys. It cannot even be hacked by future quantum computers, because it makes use of some special features of quantum mechanics.
There are different ways to implement QKD, but they all use photons to send the key. I will explain a method that is called BB84, because it was presented by Charles H. Bennett and Gilles Brassard in 1984. BB84 is commonly referenced as the first QKD protocol.
In BB84, photons are assigned a polarisation basis and a value. The polarisation basis (or basis) can be orthogonal (+) or diagonal (x). The value can be either 1 or 0. So the properties of the photons can be: +1, +0, x1, x0.
Computers usually express all letters or numbers through a sequence of 0 and 1. For example, the letter 'h' is encoded as 01101000. So a long sequence of photon values can represent a secret key that contains all kinds of different numbers or letters.
You (the sender) can choose which base to use to encode either the value 0 or 1 into a photon. However, due to quantum phenomena, if Bob uses a different basis to read out the photon value, he will randomly read a 0 or a 1. This also alterates the photon irrevocably and its original state gets lost.
To simulate the BB84 protocol, you will now send Bob some marbles – which represent the photons – and choose their values and bases. But this is all top-secret! So don't tell anybody what configurations you choose and make sure that the padlock-shaped shields are covering the marble track! Let's start!

E.2.2 Protocol Explanation Screens Textcontents (Alice Version). Choose a random base by rotating the blue knob over the marble track. Then, send a photon with the value 0 or 1 using one of the buttons on the tower.
You can see the value and base of your photon below. However, you don't know if Bob actually measured this value. Choose a base and send the next photon!
Great! You can either send more photons manually or click on the button to send the rest automatically. [Button

text: Send Photons Automatically]
Next, you exchange your chosen bases - but only the bases, not the values! - with Bob. This does not need to be kept secret, because the qubit have already been exchanged. [Button text: Get Partner's Bases]
You can now see that you and Bob sometimes chose the same basis and sometimes did not. Press the button to highlight these instances. [Button text: Compare Bases]
Now you collect only the photon values where you and Bob used the same basis (green boxes). The values Bob measured from these photons should match what you sent. [Button text: Same Bases Only]
You next compare a specific part of the value sequence with Bob to check if they are actually the same. [Button text: Compare Some Values]
The values are the same! Now Bob and you can use the rest of the sequence as a shared secret key! [Button text: Generate Key]
This is your shared secret key, which you can use to encrypt your secret messages! If you want to, you can talk to Bob to compare it "offline", but this is not part of the BB84 protocol. But why is BB84 now so secure? [Button text: Why is it secure?]

E.2.3 Eve Introduction Screens Textcontents (Alice Version). To explain this, you will now exchange another key, but this time, someone will be listening in on your communication. Please take the padlock-shaped shield now off...
You can now see that Eve is in the middle of the marble track... She is intercepting your communication. For this, she has to also guess a base, so please use her knob to simulate this, configure your own base however you want, and send again some photons.

E.2.4 Eve Protocol Explanation Screens Textcontents (Alice Version). Choose a base and send some photons. Please remember to configure Eve's base together with Bob.
Again, choose a base and send some more photons. Make sure that Eve guesses sometimes correctly and sometimes not.
You can now again either send Bob more photons manually or send the rest automatically. [Button text: Send Photons Automatically]
Next, you publicly exchange your chosen bases with Bob. The values again remain secret, so Eve cannot intercept them! [Button text: Get Partner's Bases]
Press the button to highlight whether or not you selected the same base as Bob. [Button text: Compare Bases]
Now, let's select the photon values where you and Bob chose the same basis. [Button text: Same Bases Only] The last step is to again compare a specific part of the value sequence with Bob. [Button text: Compare Some Values]
Oh! The values are not the same because Eve influenced some when she used a different base from Bob and you! [Button text: Generate Key]
You now know that someone intercepted your key exchange and won't use this key to encrypt your messages. [Button text: Why is it secure?]

E.2.5 Final Text on Explanation Screen. So with BB84, you can detect if the exchanged key was intercepted by someone else or not. Moreover, an attacker like Eve has theoretically no way to avoid this. This is why QKD is so secure!

F COMPARISON STUDY

F.1 Statistical Analysis of Quantitative Results

Table 7. Descriptives and significance test results for all qualitative measures comparing the tangible, slides, and video. We abbreviated the One-Way ANOVA with AN and the Kruskal-Wallis test with KW. Bold values indicate the highest mean per row and statistically significant test results ($p <= 0.05$).

	Descriptives (format: Mean(Std))			Significance Test	
	tangible	slides	video	test	result
Understanding (Quiz)	4.58 (1.31)	**4.83 (2.64)**	4.30 (1.95)	AN	$F(2, 40) = 0.159$, $p = 0.854$
SUS	56.54 (17.58)	54.22 (15.16)	**58.75 (15.74)**	AN	$F(2, 40) = 0.296$, $p = 0.745$
RTLX	38.78 (13.59)	34.90 (17.66)	**48.45 (22.23)**	AN	$F(2, 40) = 2.142$, $p = 0.131$
UEQ-S Overall	**1.10 (0.94)**	0.68 (1.11)	0.96 (1.22)	–	–
UEQ-S Hedonic Quality	**1.85 (0.56)**	0.81 (1.18)	0.93 (1.49)	KW	$\mathbf{H(2, 43) = 6.089, p = 0.048}$
UEQ-S Pragmatic Quality	0.35 (1.56)	0.55 (1.27)	**1.00 (1.13)**	AN	$F(2, 40) = 0.883$, $p = 0.421$
UES-SF Aesthetic Appeal	**3.64 (0.71)**	3.48 (0.57)	3.40 (0.96)	KW	$H(2, 43) = 1.264$, $p = 0.531$
UES-SF Focused Attention	**3.62 (0.68)**	2.94 (0.55)	3.24 (0.93)	AN	$F(2, 40) = 3.106$, $p = 0.056$
UES-SF Perceived Usability	3.08 (0.73)	3.25 (0.83)	**3.33 (0.89)**	KW	$H(2, 43) = 0.662$, $p = 0.718$
UES-SF Reward Factor	**4.00 (0.86)**	3.65 (0.65)	3.83 (0.98)	KW	$H(2, 43) = 2.889$, $p = 0.236$
IMI Interest/Enjoyment	**5.21 (1.07)**	4.58 (1.13)	4.17 (1.22)	KW	$\mathbf{H(2, 43) = 5.995, p = 0.050}$
IMI Perceived Competence	3.87 (1.41)	3.98 (1.12)	**4.13 (1.55)**	AN	$F(2, 40) = 0.124$, $p = 0.884$
IMI Value/Usefulness	**5.19 (1.25)**	4.80 (1.20)	4.67 (1.06)	KW	$H(2, 43) = 2.682$, $p = 0.262$
HCTS Benevolence	**3.59 (0.60)**	3.40 (1.11)	3.50 (0.55)	KW	$H(2, 43) = 0.035$, $p = 0.983$
HCTS Competence	4.13 (0.42)	3.54 (0.93)	**4.21 (0.58)**	KW	$\mathbf{H(2, 43) = 7.405, p = 0.025}$
HCTS Perceived Risk	2.15 (0.66)	**2.85 (0.85)**	2.55 (0.90)	KW	$H(2, 43) = 4.140$, $p = 0.126$
HCTS Reciprocity/Trust	3.54 (0.80)	3.54 (0.85)	**3.81 (0.52)**	KW	$H(2, 43) = 0.840$, $p = 0.657$