Power System Technology
ISSN:1000-3673

Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

Quantum Cryptography, Its Learning, Simulation and Algorithm

Mohd Nazeer[1], Mohammed Qayyum[2], S sathappan[3], Gouri patil [4] , Venkata Subbareddy[5]

[1,5]*Associate Professor, Vidya Jyothi Institute of Technology, Hyderabad, India*

[2]*Department of Computer Science & Engineering, King Khalid University, Saudi Arabia..*

[3]*Associate Professor, Rajalakshmi engineering college, Chennai*

[4]*Muffakhamjah College of Engineering and Technology, Hyderabad, India.*

mohdnazeerai@vjit.ac.in

mgiwm@kku.edu.sa

sathappan.s@rajalakshmi.edu.in

gouripatil@mjcollege.ac.in

kvsreddy2012@gmail.com

Abstract:- Quantum computing and cryptography are rapidly emerging as significant fields due to their potential to transform computation and secure communication. However, many existing learning platforms are fragmented, technically complex, and primarily designed for advanced users, with the acknowledge of basic computing, statistics security, networking and quantum physics mandatory to understand. To address this challenge, this research article presents Quantum simulator, a web-based integrated educational and simulation platform developed to simplify the learning of quantum computing and cryptographic security, navigates the transition to a quantum security framework, offering a critical analysis of encryption methods essential for the protection of critical infrastructure in the quantum era. The platform integrates theoretical learning modules, explanations of quantum algorithms, a visual quantum circuit simulator, automatic OpenQASM code generation, a BB84-based Quantum Key Distribution (QKD) simulator, documentation support, analytics, a Help and Complaints Section for user support, a chatbot for interactive query resolution, and a comparative module for classical and quantum computing. The system follows a layered web architecture that supports content delivery, simulation processing, and user interaction. Functional evaluation of the major modules demonstrates the feasibility of integrating conceptual learning, circuit design, cryptographic simulation, and learner assistance within one comprehensive platform. The results indicate that the proposed approach can enhance accessibility, conceptual clarity, practical engagement, and guided learning support for early-stage learners in quantum technologies. This paper not only forecasts quantum threats but also offers a sophisticated, actionable framework for strengthening infrastructure and algorithm model code for environments against the multifaceted challenges of the quantum era.

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

Keywords: *Quantum Computing, Quantum Cryptography, Cryptographic techniques, BB84 Protocol, Quantum Simulation.*

1. Introduction

The rise of quantum computing represents a paradigm shift in the form of cyber security. Quantum computing's significant implications infiltrate every layer of our digital infrastructure, casting a shadow of hesitation over the area of cybersecurity [1]. Quantum computing has emerged as a powerful computational paradigm that exploits the principles of superposition, entanglement, and quantum interference to solve certain classes of problems more efficiently than classical computing [2]. At the same time, quantum cryptography has gained considerable importance because it offers new approaches to secure communication, particularly through quantum key distribution protocols such as BB84. As research and industrial interest in quantum technologies continue to grow, there is an increasing need for learning environments that make these concepts accessible to students and beginners [3].

Although a number of quantum platforms and software frameworks are available today, many of them are aimed at researchers, developers, or experienced learners. Tools such as Qiskit, Azure Quantum, and other circuit-based simulators provide significant technical capabilities, but they often require prior familiarity with programming, quantum mechanics, and mathematical foundations [4]. In addition, learning materials, algorithm visualizations, circuit simulation, cryptographic demonstrations, learner support, and doubt clarification are often distributed across separate tools and resources [5]. This fragmented approach creates a steep learning curve for users who are beginning to explore the domain.

For learners and early-stage researchers, the absence of a unified and beginner-oriented platform becomes a serious limitation. A user interested in learning quantum gates, quantum cryptography, building a circuit, understanding quantum key distribution [6], comparing classical and quantum approaches, resolving doubts instantly, and reporting platform-related issues may need to rely on multiple disconnected systems. As a result, conceptual continuity is lost, practical engagement becomes more difficult, and the learning experience becomes less interactive.

1.1 Quantum Simulator

To address this gap, this paper proposes Quantum simulator, an integrated web-based platform that combines theory, simulation, visualization, cryptographic learning, chatbot-based doubt clarification, and user support into a single educational environment. The system is designed to support beginners through structured modules that explain algorithms, allow visual quantum circuit construction, generate corresponding Open QASM code, simulate BB84-based key distribution, provide a chatbot for answering user questions, include a Help and Complaints Section for support and issue reporting, and present comparisons between classical and

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

quantum computing. The goal of the proposed system is not only to provide technical functionality but also to improve accessibility, clarity, learner guidance, and interactive learning in quantum education.

1.2 Quantum Cryptography

A. Motivation

Building upon the insights presented in the introduction, this research is motivated by the imperative to address the profound cybersecurity challenges brought forth by the rapid advancements in quantum computing, especially within encryption and security services. Quantum computing, with its potential for exponentially greater computational power, represents a tough threat to traditional cryptographic methods, which are foundational to the security of data in terms of its integrity, confidentiality, and availability. our research not only addresses an urgent need in the face of emerging quantum threats but also contributes vital insights to the broader discourse on protecting our interconnected digital world. This research, therefore, stands as a crucial step in preparing and learning gates and security algorithms.

B. Contribution

This research article significantly contributes to the domain of cyber security in the era of quantum computing, focusing on the development and understanding of quantum gates and measures. The key contributions include: In-Depth Analysis across gates: Our exhaustive examination provides a multi-layered analysis of the potential security threats emerging from quantum computing.

These contributions collectively mark a significant advancement in securing infrastructures against quantum computing threats. They provide vital insights and methodologies for stakeholders, shaping the development of quantum-resistant security measures, guiding infrastructure adaptation, and influencing policy decisions. Therefore, this paper plays a critical role in enriching the security posture of networked systems in anticipation of quantum computing advancements.

The main contribution of this work lies in the development of a unified educational framework that connects conceptual understanding with practical interaction. By bringing together multiple learning, simulation, assistance, and support components in one platform, Quantum simulator aims to serve as a bridge between theoretical quantum knowledge and hands-on exploration.

C. Organization

This paper is organized as follows: Section II provides a background of quantum computing and cybersecurity, with a focus on quantum cryptographic methods. Section III provides implementation details of the simulator with its limitation. It explains the complete workflow

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

of the simulator with the help of the diagram. Section IV discusses the system architecture in detail description of each and every module of the quantum crypto simulator and cyber security. Section V result and discussions about the implementation steps of implementing various cyber security algorithm in details. Section VI with a summary and future research directions, offering consolidated insights into the role of quantum computing in cybersecurity

2. Litetature Survey

The theoretical foundations of quantum computing were established through the pioneering work of Feynman and Deutsch [1]. Feynman argued that classical systems are inherently inefficient for simulating quantum phenomena and suggested that computation based on quantum mechanical principles would be more suitable for such tasks. [7] Deutsch later formalized the concept of a universal quantum computer, providing a theoretical basis for quantum computation as a distinct computational model.

The section also highlights gaps in current research, particularly in addressing the gates and complexity of quantum cyber threats to both present and future. This section comprehensively reviews the advancements in quantum computing, the evolution of quantum cryptography, and their collective impact on digital infrastructure and cybersecurity. The quantum crypto simulator emphasizes the transition of quantum computing from theoretical concepts to applications that directly challenge traditional cryptographic algorithms. [8] highlights the critical need for a quantum resistant direction in cybersecurity, including the anticipation of timelines for certifying quantum-resistant standards and preparation against potential quantum attacks. [9] propose a comprehensive framework highlighting a systematic shift to post-quantum cryptography, highlighting the need for robust testing, well-planned integration timelines, and a thorough strategy for achieving quantum-safe enterprise systems in response to the challenges posed by quantum computing. [10] provide a comprehensive survey of Quantum Cryptography for Enhanced Network Security and future directions in this domain. These represent an effort to navigate the evolving cybersecurity landscape in the quantum era.

2.1 Evolution of Quantum Computing and Cryptography

Recent advancements in quantum computing technology, by different vendors such as IBM and google, prove an accelerated approach towards practical applications, under scoring the urgency of post quantum cryptography development [11], [12], [13]. Quantum computing has quickly moved from theoretical exploration to practical applications, with major implications in the field of cryptography. The groundbreaking work by Shor [7] [14] revealed the vulnerability of conventional cryptographic protocols, such as ECC and RSA, against quantum computing attacks, specifically how quantum algorithms could exploit mathematical shortcuts for breaking these systems. This breakthrough has provided the development of PQC, which is focused on designing algorithms secure against both classical and quantum computing threats.

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

The contributions by [15] in providing latest algorithmic paradigms have further enriched this domain, including developments in algorithm quickness and adaptability.

2.2 Gaps in Current Research and Our Focus

While there has been significant progress in PQC and understanding the broader implications of quantum computing theoretically, there remains a critical gap in detailed analyses and implementation of quantum induced cyber threats, particularly those affecting existing and future gates. Previous research has mostly centered on theoretical general aspects of PQC and quantum computing's implications, often missing the finer details of these emerging challenges and practical implementation of it. Our research aims to fill this gap, by providing simulator to have hands of experience of various gates and algorithm related to cyber security and cryptography.

Over time, quantum algorithms demonstrated the practical significance of this computational paradigm. Shor's algorithm showed that quantum computers could perform integer factorization and discrete logarithm computations far more efficiently than known classical methods, thereby threatening widely used public-key cryptographic systems such as RSA. [16] further demonstrated that quantum search could provide quadratic speedup for unstructured search problems. These developments established quantum computing as both a technological opportunity and a security challenge. In the area of quantum cryptography, [17] introduced the BB84 protocol, which became the first major quantum key distribution scheme.[18][19] BB84 demonstrated that the laws of quantum mechanics could be used to establish secure communication and detect eavesdropping attempts. Subsequent work by [20][21] expanded the theoretical and practical understanding of QKD security, implementation challenges, and protocol robustness. This made QKD one of the most important practical applications of quantum information science.

Several software platforms have significantly improved access to quantum programming and simulation. [4] IBM's Qiskit provided an open-source framework for constructing and simulating quantum circuits, while tools such as Quirk and Azure Quantum introduced graphical and cloud-based environments for experimentation [22][23]. These platforms are valuable for research and development; however, they are often optimized for technically skilled users rather than beginners. Most existing systems focus primarily on circuit construction or execution and do not fully integrate educational guidance, cryptographic demonstrations, and comparative conceptual learning in a single environment.

Educational research has consistently shown that interactive and experiment-driven learning environments can improve conceptual understanding more effectively than passive content delivery. In the context of quantum learning, this indicates the need for platforms that support both explanation and exploration. Despite the availability of powerful individual tools, there

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

remains a gap for a beginner-oriented, web-based system that combines algorithm learning, circuit simulation, code generation, and QKD-based cryptographic understanding in a unified framework.

Based on this gap, the present work proposes Quantum simulator as an integrated educational and simulation platform. Unlike existing tools that address isolated aspects of quantum learning, the proposed system aims to combine foundational concepts, practical circuit interaction, [24] BB84-based simulation, and comparative learning support into one coherent environment for students and early-stage learners.

3. Quantum Crypto Simulator

This work proposes Quantum simulator, a web-based learning and simulation platform designed to provide an integrated environment for studying quantum computing and quantum cryptography. The system is intended primarily for beginners, students, and early-stage learners who require a simplified yet structured interface for understanding both conceptual and practical aspects of quantum technologies.

The proposed platform addresses a key limitation of many existing resources: the separation of educational content, simulation tools, cryptographic demonstrations, learner assistance, and user support across multiple systems. Instead of forcing users to shift between different learning environments, Quantum simulator combines multiple functionalities into a unified framework. This allows users to progress from theoretical understanding to practical interaction within the same platform.

The system includes several core modules. The dashboard serves as the central navigation point for accessing all available sections. The algorithms module presents major quantum algorithms along with their purpose, conceptual background, and circuit-level understanding. The learning modules provide topic-wise explanations of fundamental and intermediate concepts such as qubits, quantum gates, measurement, superposition, entanglement, and cryptographic foundations.

A major component of the platform is the quantum simulator, which enables users to visually construct quantum circuits using gate-based interaction. The platform also supports circuit-to-code generation, through which the designed circuit is automatically converted into its equivalent Open QASM representation. This strengthens the connection between graphical learning and code-level understanding.

[25] Another key contribution of the system is the BB84-based Quantum Key Distribution simulator, which demonstrates the process of basis selection, qubit transmission, measurement comparison, and secure key establishment. By including this module, the platform extends beyond algorithm learning and introduces users to practical quantum cryptographic principles in an accessible form.

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

In addition to these learning and simulation modules, the platform includes a chatbot section that enables users to ask questions related to quantum computing, cryptography, and platform usage, and receive instant responses [26][27]. This feature improves interactive learning by providing immediate doubt clarification within the same environment. The system also contains a Help and Complaints Section, which allows users to report issues, seek assistance, and communicate difficulties encountered while using the platform. These features improve usability, learner support, and user-centred interaction.

Furthermore, the platform includes documentation, analytics, and a quantum vs classical comparison module. These features improve conceptual reinforcement, usability, and overall learning continuity. Through this integrated design, Quantum simulator aims to provide a beginner-friendly educational system that combines theoretical explanation, simulation, cryptographic application, instant assistance, and support services in a single web-based platform.

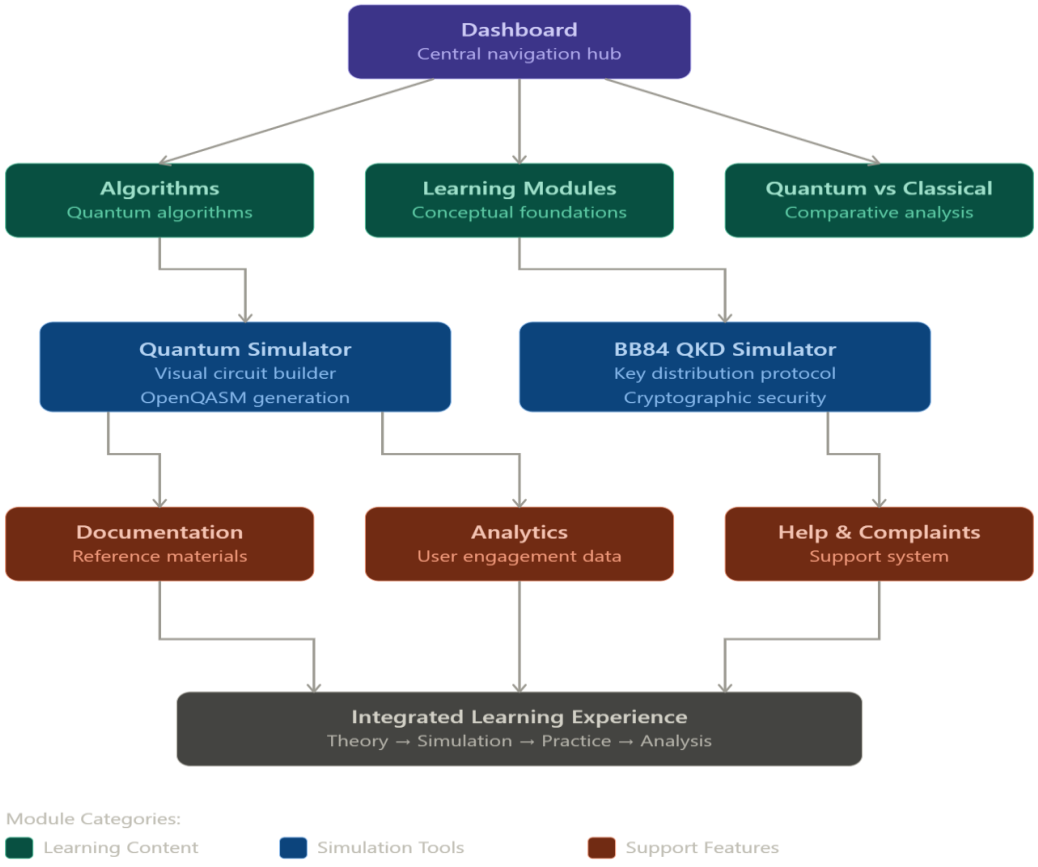


Fig 3.1: Operational Workflow of the Proposed Quantum simulator Platform

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

4. Simulator Architecture

The architecture of Quantum simulator follows a layered web-based model designed to support content delivery, simulation handling, user interaction, learner assistance, and support services in an organized and scalable manner. The system is structured into three primary layers: the user interaction layer, the application processing layer, and the content and data layer.

The user interaction layer forms the front-end interface through which learners access the platform. It includes the dashboard, algorithms section, learning modules, simulator interface, QKD module, chatbot section, analytics view, help and complaints section, and quantum vs classical comparison module. This layer is responsible for providing an intuitive and beginner-friendly experience, enabling users to navigate the platform and interact with its modules without requiring advanced technical knowledge.

The application processing layer acts as the core logical component of the system. It manages user requests, controls navigation across modules, processes circuit-building actions, generates Open QASM code, handles BB84 simulation flow, manages chatbot query-response interaction, and coordinates analytics and support functionalities. This layer ensures that user interactions are translated into appropriate responses and computational outputs. It also plays an important role in maintaining consistency between the educational content, learner assistance mechanisms, and the practical simulation environment.

The content and data layer stores the learning resources, algorithm descriptions, simulator configurations, chatbot knowledge content, documentation materials, analytics-related information, and support-related data used by the system. This layer enables structured retrieval of content and supports the functioning of both the educational and interactive components of the platform. By separating storage from processing and interface logic, the architecture promotes modularity and future scalability.

Overall, the layered architecture ensures that Quantum simulator remains organized, maintainable, and extensible. It allows educational content, simulation logic, chatbot-based learner support, issue-handling features, and user interaction to function together within a unified framework while still supporting future expansion such as real quantum hardware integration, additional algorithms, and more advanced cryptographic simulations.

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

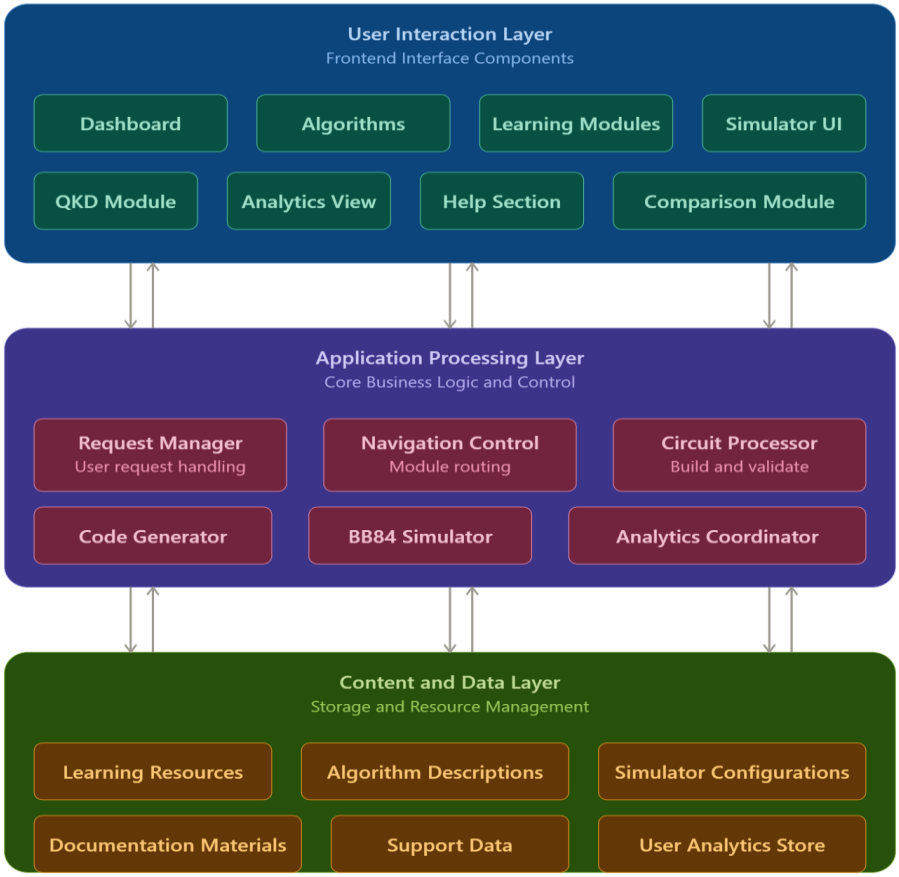


Fig 4.1: System Architecture of the Proposed Quantum simulator Platform

5. Results And Discussions

The proposed Quantum simulator platform was successfully implemented as a web-based environment for learning and interacting with quantum computing and quantum cryptography concepts. The developed system integrates theoretical content, visual circuit construction, OpenQASM code generation, BB84-based simulation, chatbot-assisted query support, help and complaints functionality, and comparative learning support into a single interface. The implementation demonstrates the feasibility of creating a unified educational platform that connects conceptual understanding with practical experimentation and learner assistance.

One of the major outcomes of the platform is the successful integration of multiple learning components that are often found separately in existing tools. Through the dashboard, users can access algorithms, learning modules, simulator features, QKD simulation, documentation, analytics, chatbot assistance, and support services in a continuous workflow. This integrated

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

structure improves usability and reduces the fragmentation that typically affects beginner-level learning in quantum technologies.

The simulator module functions as an important bridge between theory and implementation. Users can visually construct simple quantum circuits and observe their corresponding OpenQASM code. This confirms the platform's ability to translate graphical interaction into code-level representation, thereby supporting both conceptual and technical learning. Similarly, the BB84-based QKD simulator demonstrates the secure key exchange process in an understandable and interactive manner, making quantum cryptography more accessible to learners.

The chatbot feature further improves the learning experience by enabling users to ask questions and obtain immediate responses related to quantum concepts, cryptographic topics, and platform usage. In addition, the Help and Complaints Section strengthens user-centered support by allowing issue reporting and assistance requests. Together, these modules improve guided learning, practical usability, and learner confidence.

The implemented results indicate that the system is effective as an introductory educational platform. Its design supports gradual learning, visual exploration, practical interpretation of concepts, interactive doubt clarification, and structured user support. While the present work focuses primarily on functional integration and educational accessibility, the platform establishes a strong foundation for future extensions involving deeper performance evaluation, larger user studies, and hardware-based execution support.

The following subsections describe the major implemented features of the platform and discuss their educational relevance.

5.1 Graphical User Interface

The graphical user interface of Quantum simulator was designed with a focus on simplicity, clarity, and structured navigation. Since the primary target users are beginners and undergraduate learners, the interface avoids excessive complexity and instead emphasizes smooth access to major platform modules. The dashboard acts as the central entry point, allowing users to move easily between learning content, simulations, comparisons, and support sections.

The interface also supports visual interaction with circuit-based components and educational materials. This is important because quantum concepts are often difficult to understand through text alone. By combining structured layout with interactive visual design, the GUI improves accessibility and contributes to a more engaging learning experience.

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

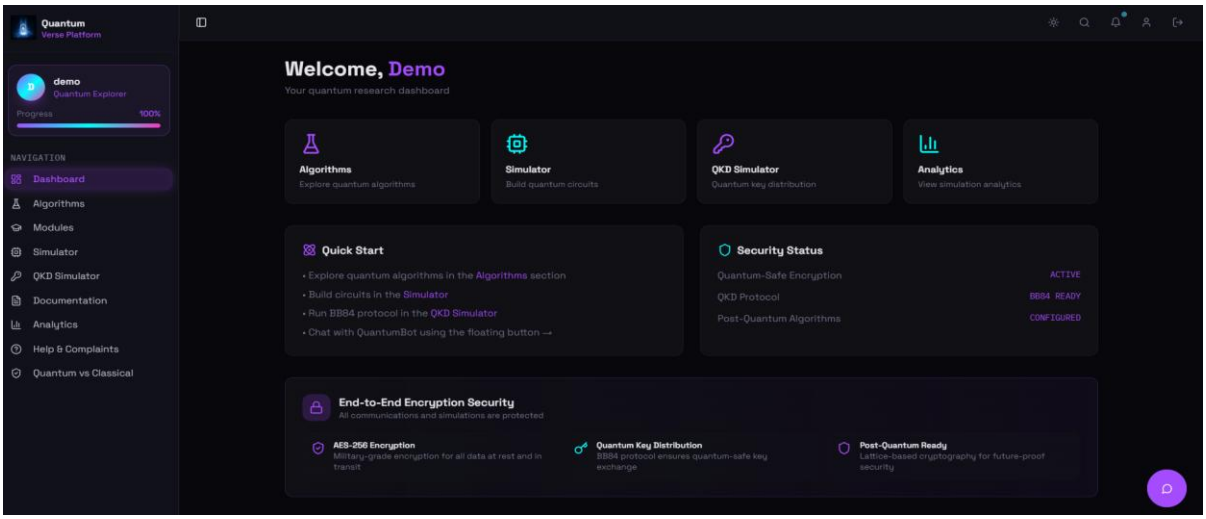


Fig 5.1: Dashboard Interface of Quantum simulator

5.2 Feature 1 – Algorithms Section

The Algorithms section presents major quantum algorithms in a structured and understandable form. Instead of treating algorithms as isolated code examples, the module explains their purpose, conceptual basis, and circuit-level significance. This approach helps learners understand not only how an algorithm is represented, but also why it is important in the broader context of quantum computing.

This section strengthens theoretical understanding and acts as a foundation for later practical interaction in the simulator. As a result, it supports a progressive learning flow from concept to implementation.

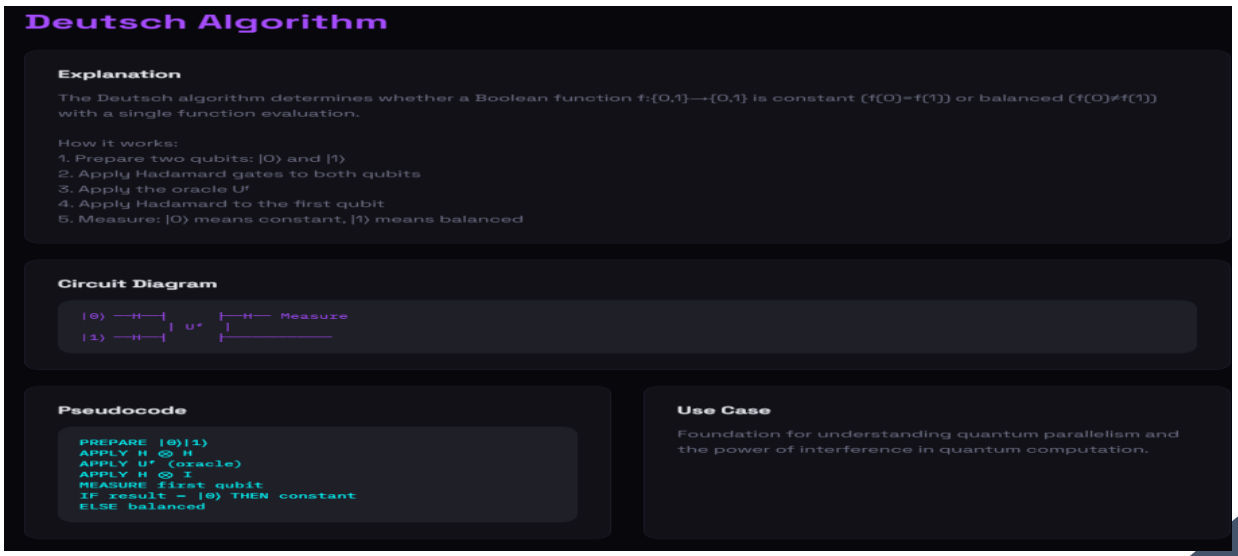


Fig 5.2: Algorithms Section of Quantum simulator

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

5.3 Feature 2 – Learning Modules

The Learning Modules section provides topic-wise educational content covering foundational and intermediate areas of quantum computing and cryptography. Concepts such as qubits, gates, measurement, superposition, entanglement, and basic cryptographic principles are introduced in a gradual and organized manner. This is especially valuable for beginners who require step-by-step exposure rather than direct entry into advanced tools. By organizing content into structured modules, the platform promotes conceptual continuity and reduces the cognitive burden associated with fragmented external learning resources.

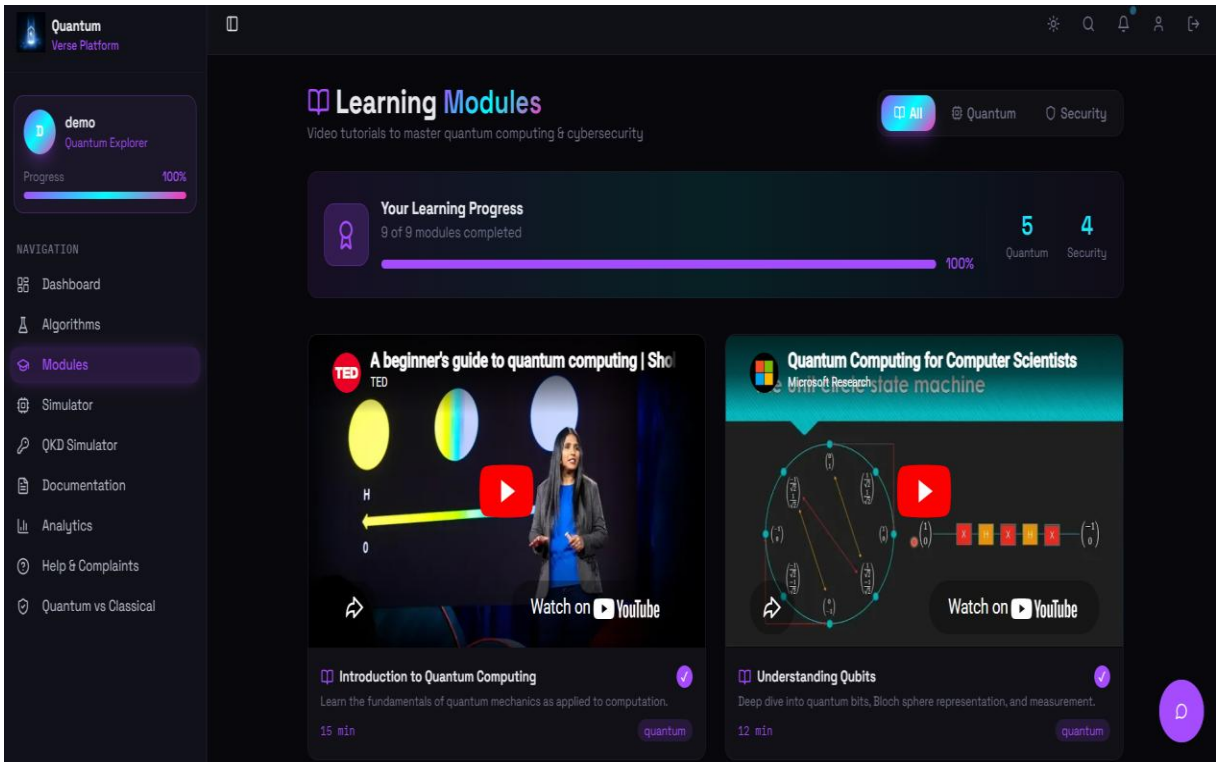


Fig 5.3: Learning Modules Interface

5.4 Feature 3 – Quantum Simulator

The Quantum Simulator is one of the core components of the platform. It enables users to construct circuits visually through gate selection and placement, thereby making circuit design more accessible for non-expert learners. Instead of requiring direct programming from the beginning, the simulator allows users to understand circuit composition through interaction. This feature is educationally important because it transforms abstract gate operations into visible structures. It also serves as a practical bridge between learning modules and code representation.

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

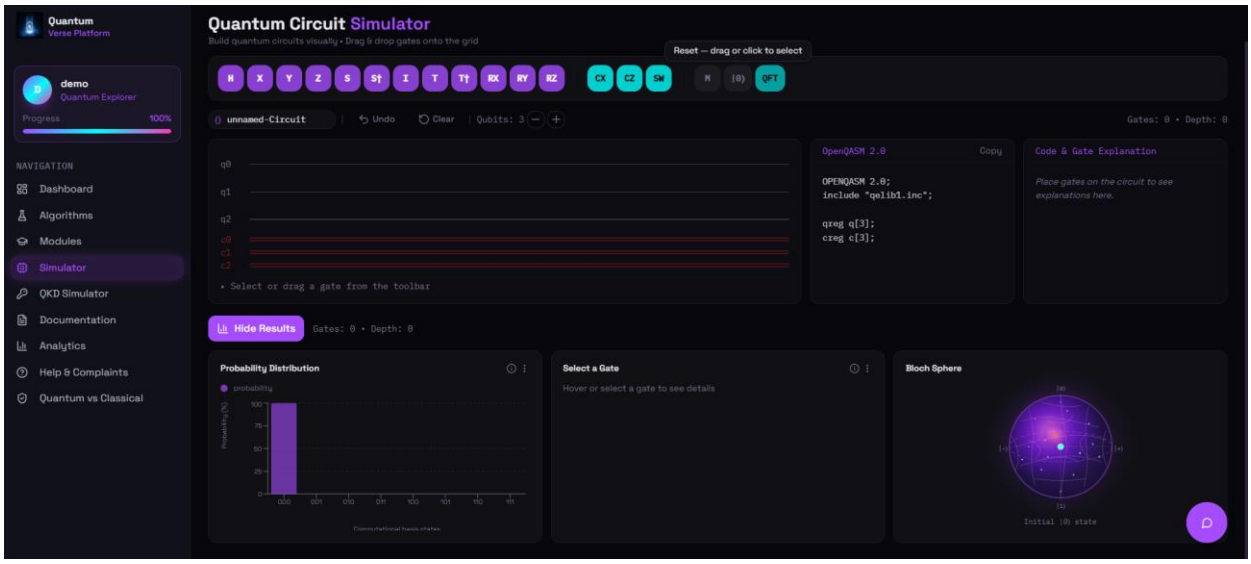


Fig 5.4: Quantum Simulator with Circuit-to-Code Output

5.5 Feature 4 – Basic Circuit Representation

The platform successfully supports circuit-to-code conversion through automatic OpenQASM generation. When users construct a basic circuit, such as placing a Hadamard gate followed by measurement, the system produces the equivalent OpenQASM code representation. This confirms that the simulator is not limited to visual demonstration alone, but also supports a more technical understanding of circuit implementation. This feature is particularly useful for learners transitioning from visual exploration to formal quantum programming frameworks.

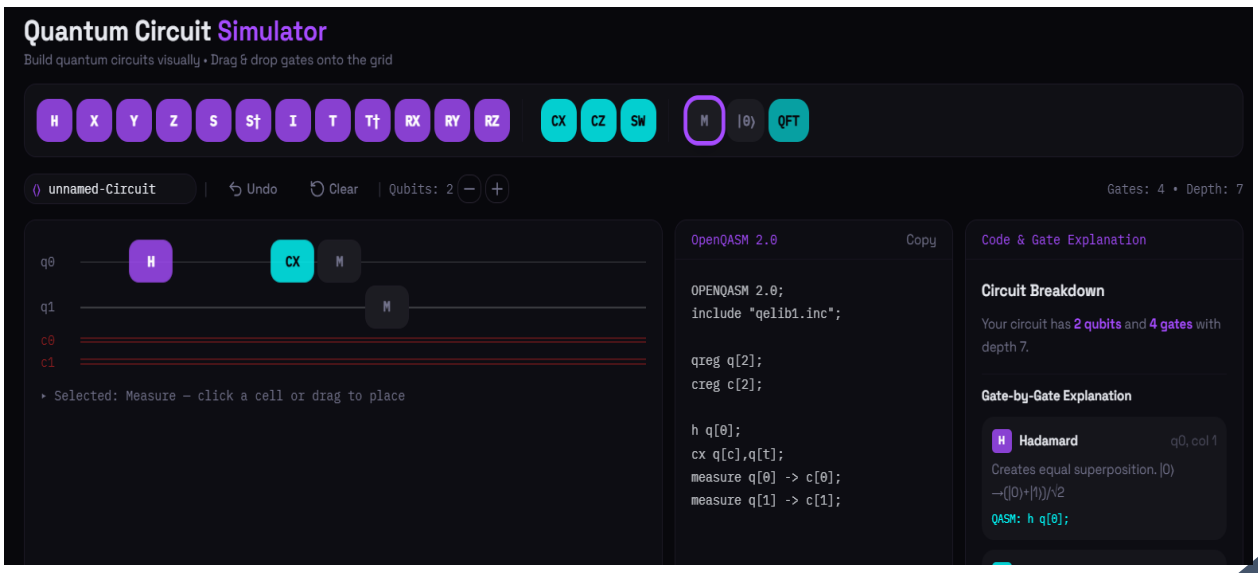


Fig 5.5: Basic Quantum Circuit and Generated OpenQASM Code

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

5.6 Feature 5 – QKD Simulator

The QKD Simulator demonstrates the working principles of the BB84 quantum key distribution protocol. Users can observe how basis selection, qubit transmission, measurement, and basis comparison contribute to secure key generation. This gives the platform a significant practical dimension, as it introduces not only computation but also cryptographic security.The educational value of this module lies in its ability to convert an otherwise highly theoretical communication protocol into an understandable and interactive learning experience.

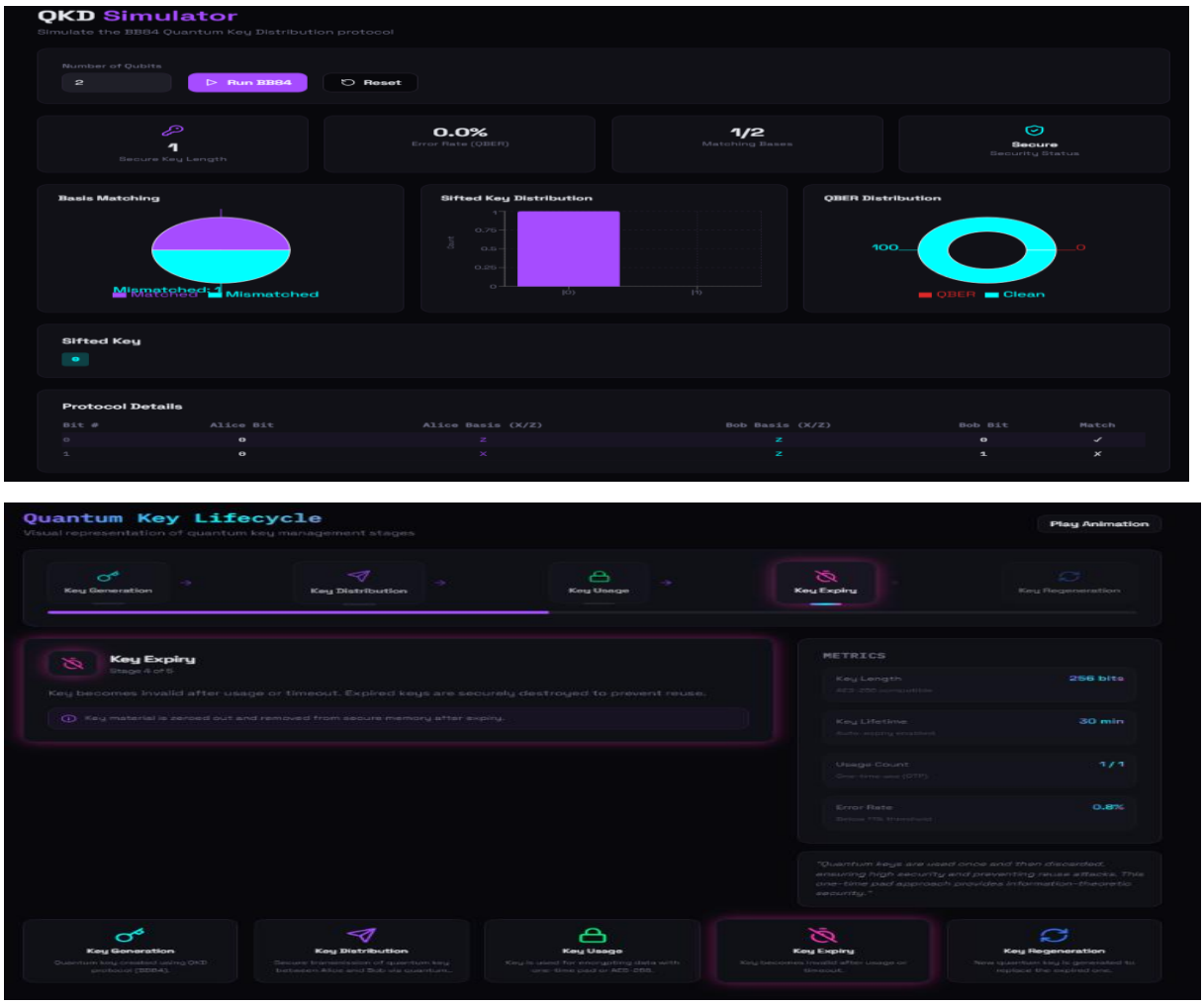


Fig 5.6: BB84-Based QKD Simulation Output

5.7 Feature 6 – Documentation Section

The Documentation section serves as a structured knowledge base for the platform. It provides users with explanations related to the project, architecture, operational flow, and theoretical foundations. This section supports learners who require more detailed clarification beyond the

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

interface-level features. From an academic perspective, this module improves transparency and strengthens the platform's role as both a learning environment and a reference system.

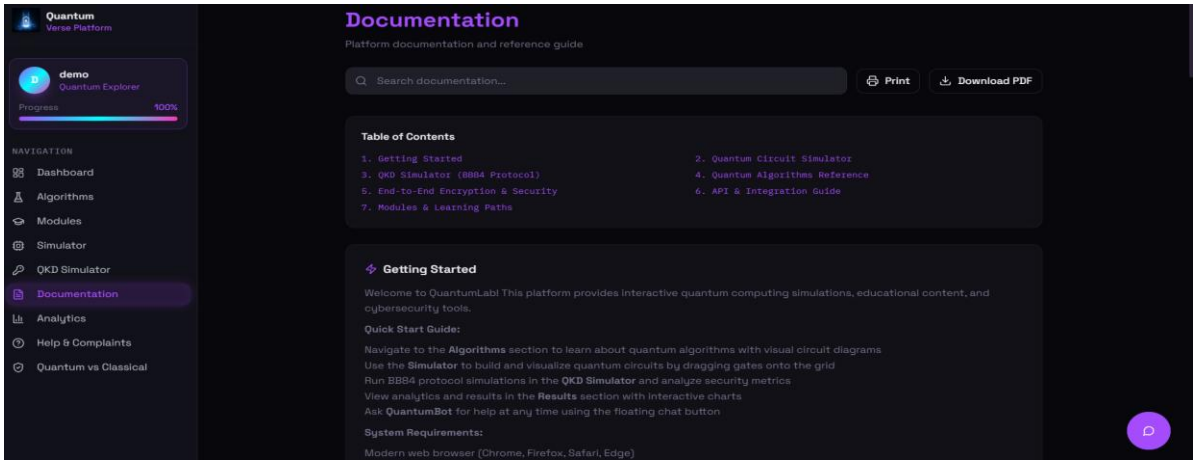


Fig 5.7: Documentation Section of Quantum simulator

5.8 Feature 7 – Analytics Section

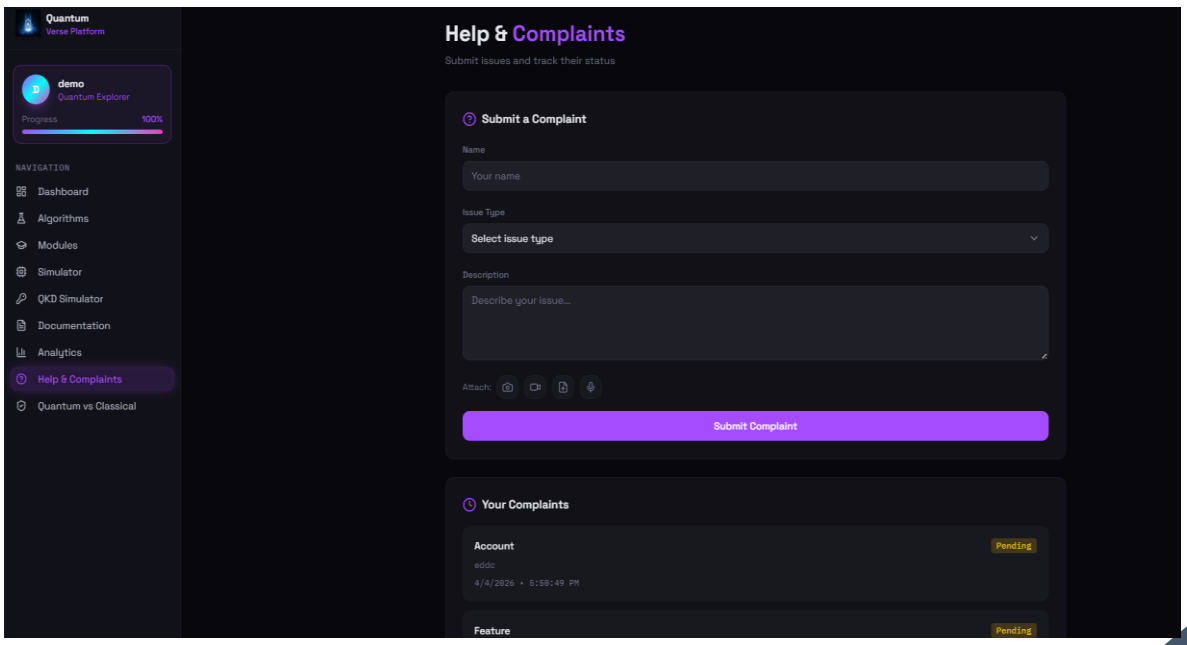
The Analytics section presents simplified insights into user engagement and platform interaction. Although the current implementation is introductory in scope, this module demonstrates how learner activity and feature usage can be observed and interpreted. Such monitoring can become useful in future educational studies, especially when evaluating which modules are most effective for concept retention and user engagement. This feature therefore adds a foundation for future data-driven improvement of the platform.

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

Fig 5.8: Analytics Section of Quantum simulator

5.9 Feature 8 – Help and Complaints Section

The Help and Complaints Section improve the user-oriented nature of the platform by providing a structured mechanism for communication, issue reporting, feedback submission, and clarification requests. Since beginner learners often encounter conceptual and technical difficulties, such a support feature contributes to overall platform usability and responsiveness. This section also strengthens the practical completeness of the platform by showing that the system is designed not only for content delivery, but also for guided learner support and issue resolution.



Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

Fig 5.9: Help and Complaints Section of Quantum simulator

5.10 Feature 9 – Quantum VS Classical Section

The Quantum vs Classical section presents a comparative understanding of classical and quantum computing. It explains key differences in information representation, processing principles, computational power, and cryptographic relevance. This module is especially useful for beginners because it helps them understand why quantum computing is fundamentally different from the classical paradigm. By placing both approaches side by side, the platform improves conceptual clarity and reinforces the significance of quantum computing in modern security and computational research.

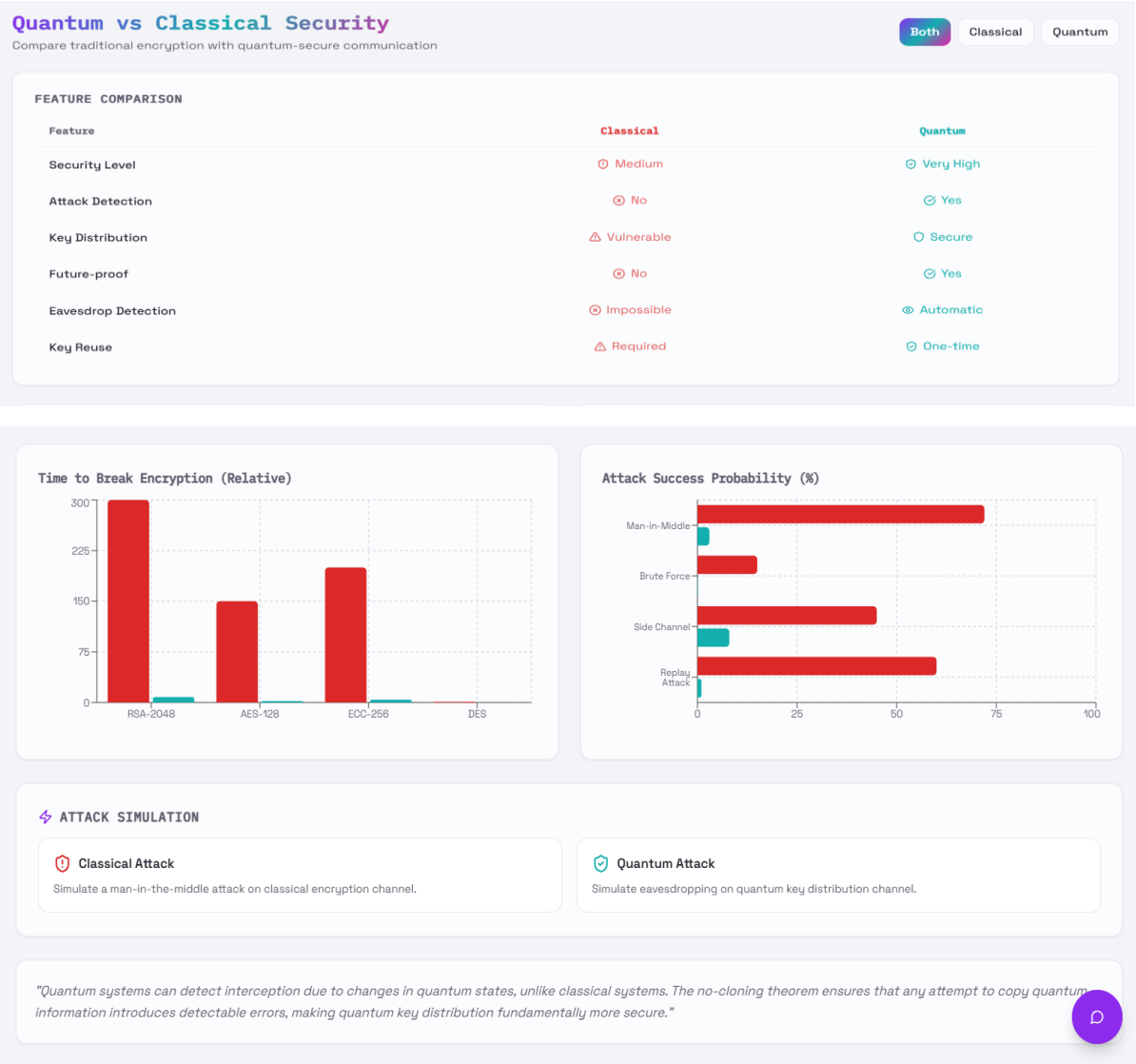


Fig 5.10: Quantum vs Classical Comparison Section

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

5.11 Feature 10 – Chatbot Section

The Chatbot Section provides an interactive support mechanism through which users can ask questions related to quantum computing, cryptography, algorithms, and platform usage. It enables users to receive instant responses within the platform, thereby improving learner engagement and doubt clarification. Instead of depending entirely on external resources, users can directly interact with the chatbot to strengthen their understanding and resolve questions in real time. This feature enhances the platform's educational value by making learning more dynamic, guided, and user-friendly.

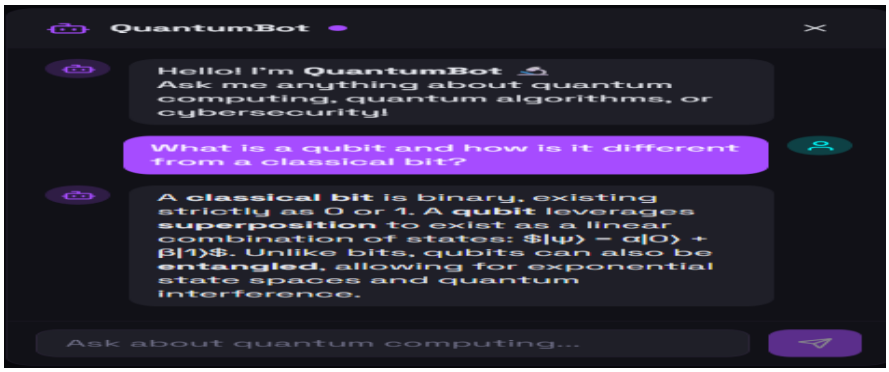


Fig 5.11: Chatbot Section of Quantum simulator

5.12 Quantum versus classic cryptography

The comparison between the quantum threat to classic cryptography by various experts is as shown below in the figure

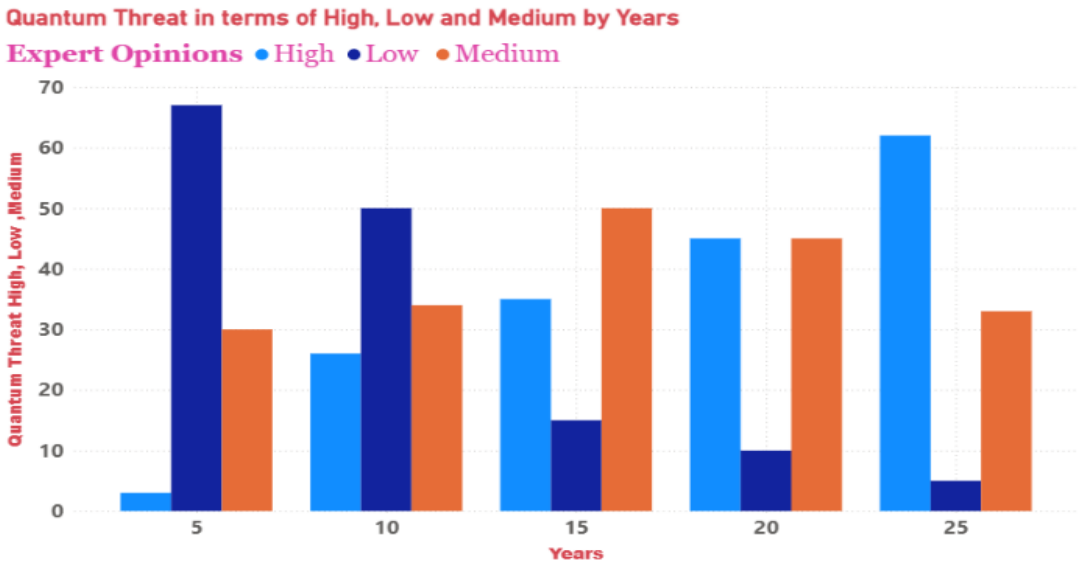


Fig : 5.12 Quantum Threat to Classic Cryptography opinions by cumulative expert

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

Figure 5.12 summarizes this evolution, incorporating insights from multiple quantum experts regarding the quantum threat timeline [28]. The "quantum threat" defined as the possibility of breaking RSA-2048 within 24 hours using a quantum machine. These assessments can be extended to evaluate the likelihood of breaking other cryptographic algorithms based on their quantum security level, as presented in Figure 5.12.

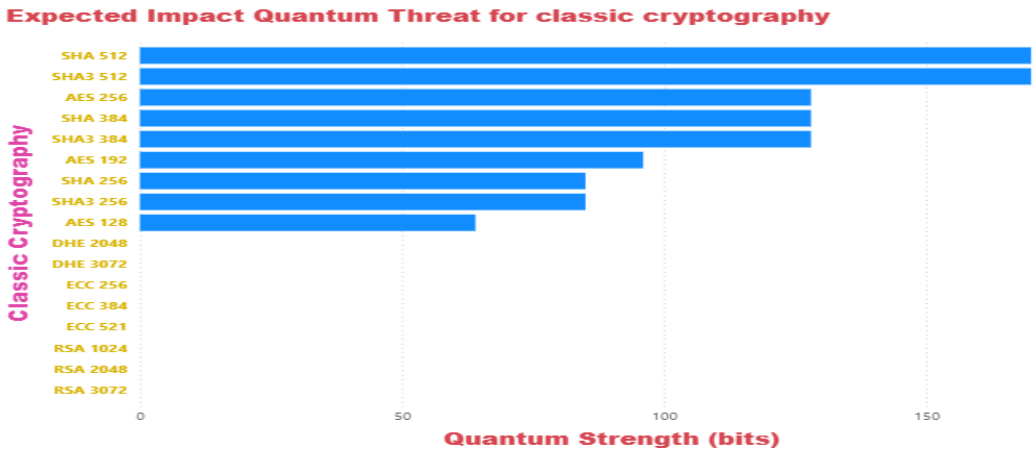


Fig: 5.13 Quantum Threat impact for classic cryptography

Quantum Impact Assessment:

we estimate the impact of quantum threats on various classic cryptographic algorithms. To conduct a classic algorithmic level risk assessment. The impact is determined based on the quantum security strength of each classic algorithm, as illustrated in Figure 5.13. An impact is considered high if the algorithm's quantum strength is less than 64 bits, low if it is greater than or equal to 128 bits, and medium if it falls between these values. The final risk assessment combines both the likelihood and impact.

6. Conclusion

The Quantum simulator, an integrated learning and simulation platform for quantum computing and cryptographic security. The system was developed to address the fragmentation and technical difficulty often associated with existing quantum learning resources. By combining educational modules, algorithm explanations, visual circuit simulation, OpenQASM generation, BB84-based QKD simulation, documentation, analytics, and comparative learning support within a single environment, the proposed platform provides a more accessible and structured experience for beginners. The implementation results demonstrate that it is feasible to unify theoretical understanding and practical interaction in one platform. Quantum crypto simulator supports learners in moving from conceptual knowledge to hands-on experimentation without requiring them to rely on multiple disconnected tools. In this way, the platform contributes to beginner-oriented quantum education by improving

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

accessibility, engagement, and conceptual continuity. Overall, the proposed work highlights the value of integrated and interactive educational environments in emerging technological domains. Quantum simulator can serve as a useful foundation for future educational platforms that aim to make advanced topics in quantum computing and cryptography more approachable for wider learner communities.

This research article has highlighted PQ cryptography represents a comprehensive, collaborative effort to protect our digital domains against upcoming quantum, the multifaceted challenges needed to safeguard against emerging quantum threats. The transition to PQ cryptography extends beyond merely adopting larger keys and ciphertexts; it dictates a fundamental reshaping of our security architectures. Addressing these vulnerabilities requires more than algorithmic updates; it demands a holistic and proactive security renovation. This collective effort should not only focus on developing and standardizing resilient PQ algorithms but also on reevaluating our overall security postures.

7. Future Scope

The scope of Quantum Crypto simulator lies in expanding it into a comprehensive and practical ecosystem for quantum computing and cybersecurity research. The platform can be enhanced by integrating with real quantum hardware such as IBM Quantum to enable execution of experiments on actual quantum processors, improving accuracy and real-world relevance. It can further incorporate advanced quantum algorithms, along with the implementation of post-quantum cryptographic techniques to explore quantum-resistant security solutions. It should continue to drive algorithmic innovation, ensuring these new solutions are both secure and practically deployable. As quantum computing continues to advance, it is imperative that our suspicious not only keep pace but also anticipate and protect future vulnerabilities. Additionally, integrating Artificial Intelligence can provide personalized learning experiences and adaptive guidance, while a cloud-based architecture can ensure scalability and collaborative access. The inclusion of immersive technologies such as AR/VR can improve visualization of complex quantum concepts, and real-time cybersecurity simulations can help analyze quantum threats and defense mechanisms, ultimately transforming Quantum simulator into a powerful tool for education, research, and next-generation secure computing.

8. Refrences

[1] Charles H. Bennett, Gilles Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical Computer Science, Volume 560, Part 1, 2014, Pages 7-11, ISSN 0304-3975, https://doi.org/10.1016/j.tcs.2014.05.025.

[2] Yaser Baseri, Vikas Chouhan, Ali Ghorbani Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure, arXiv:2404.10659v1, 2024, https://doi.org/10.48550/arXiv.2404.10659

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. 12, 1012-1236 (2020)

[4] IBM Qiskit Documentation https://qiskit.org/documentation/

[5] Lo, HK., Curty, M. & Tamaki, K. Secure quantum key distribution. Nature Photon 8, 595–604 (2014). https://doi.org/10.1038/nphoton.2014.149

[6] Scarani, V., et al. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301.

[7] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.

[8] A. Mashatan, "A look at quantum resistant encryption & why it's critical," The SSL Store, 2022.

[9] W. Barker, M. Souppaya, and W. Newhouse, "Migration to post quantum cryptography," NIST National Institute of, Standards and Technology and National Cybersecurity, Center of Excellence, pp. 115, 2021.

[10] M. Shapna Akter, "Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions," arXiv e-prints, pp. arXiv–2306, 2023.

[11] Nazeer Mohd , Qayyum, M., Patil, G., Ali, M.T., Srinivas, J., Akheel, M. (2025). Stress Detection Based on ECG, GSR Signals, HR, and Behavioral Context. In: Sahni, M., Merigó, J.M., Annamaria, GL., León-Castro, E., Verma, R., Saraswat, R.N. (eds) Mathematical Modeling, Computational Intelligence Techniques and Renewable Energy. MMCITRE 2024. Lecture Notes in Networks and Systems, vol 1192. Springer, Singapore. https://doi.org/10.1007/978-981-96-1449-3_28

[12] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, no. 7779, pp. 505–510, 2019.

[13] D. Castelvecchi, "Quantum computers ready to leap out of the lab in 2017," Nature, vol. 541, no. 7635, 2017.

[14] Mohd Nazeer, Alasiry, A., Qayyum, M., Madhan, V.K., Patil, G., Srilatha, P. (2024). Enhancing cyber security in autonomous vehicles: A hybrid XG boost-deep learning approach for intrusion detection in the CAN bus. Journal Européen des Systèmes Automatisés, SCOPUS (Q3), Vol. 57, No. 5, pp. 1295-1304. https://doi.org/10.18280/jesa.570505

[15] A. Kumar and S. Garhwal, "State-of-the-art survey of quantum cryptography," Archives of Computational Methods in Engineering, vol. 28, pp. 3831–3868, 2021.

[16] A. Sharma and A. Kumar, "A Survey on Quantum Key Distribution," 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/ICICT46931.2019.8977649.

Power System Technology
ISSN:1000-3673
Received: 16-02-2026 Revised: 05-03-2026 Accepted: 26-04-2026

[17] I. W. Primaatmaja, K. T. Goh,E. Y. Z. Tan and J. T. F. Khoo, "Security of Device Independent Quantum Key Distribution Protocols: A Review,"arXiv, Jun. 2022. https://doi.org/10.48550/arXiv.2206.04960

[18] M. Shapna Akter, "Quantum Cryptography for Improved Network Security: A Survey of Research, Developments, and Future Directions," arXiv, Jun. 2023. https://doi.org/10.48550/arXiv.2306.09248

[19] Likang Zhang, Wei Li, Jiawei Pan, Yichen Lu, Wenwen Li, Zheng-Ping Li, Yizhi Huang, Xiongfeng Ma, Feihu Xu, and Jian-Wei Pan Phys. Rev. X 15, 021037 (2025)

[20] Emir Dervisevic, Amina Tankovic, Ehsan Fazel, Ramana Kompella, + 3, Peppino Fazio, Miroslav Voznak, Miralem Mehic Quantum Key Distribution Networks – Key Management: A Survey," ACM Computing Surveys, Volume 57, Issue 10 Article No.: 257, Pages 1 – 36

[21] Aitor Brazaola-Vicario, Alejandra Ruiz, Oscar Lage, Eduardo Jacob, and Jasone Astorga Quantum key distribution: a survey on current vulnerability trends and potential implementation risks Vol. 3, Issue 8, pp. 1438-1460 (2024) •https://doi.org/10.1364/OPTCON.530352

[22] Improved method for stress detection using bio-sensor technology and machine learning algorithms", Mohd Nazeer, Shailaja Salagrama, Pardeep Kumar, Deepak Parashar, Mohammed Qayyum, Gouri Patil," methodx, VOLUME 12, 102581, JUNE 2024, SCOPUS (Q2),ESCI, http://methods-x.com/article/S2215-0161(24)00035-9/fulltext

[23] R. Ramya, P. Kumar, D. Dhanasekaran, R. Satheesh Kumar, S. Amithesh Sharavan, A review of quantum communication and information networks with advanced cryptographic applications using machine learning, deep learning techniques, Franklin Open, Volume 10,2025,100223, ISSN 2773-1863, https://doi.org/10.1016/j.fraope.2025.100223.

[24] A. Kumar and S. Garhwal, "State-of-the-art survey of quantum cryp tography," Archives of Computational Methods in Engineering, vol. 28, pp. 3831–3868, 2021.

[25] P N. N. Laboratory, "Inventory of public key cryptography in us electric vehicle charging infrastructure," https://www.pnnl.gov, Tech. Rep., 2023.

[26] Mohiuddin, M. A., Nazeer, M., Patil, G., Qayyum, M., Rajab, A. S., & Ganesh, B. (2025). Stress detection based on facial expression, challenges and application using quantum computing. In Multi-Disciplinary Research and Sustainable Development (pp. 263-267). CRC Press.

[27] Ravi, S. S. Roy, A. Chattopadhyay, and S. Bhasin, "Generic side channel attacks on cca-secure lattice-based pke and kems." IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2020, no. 3, pp. 307–335, 2020..