Post-quantum trails: an educational board game about post-quantum cryptography.

Jelizaveta Vakarjuk
Cybernetica AS
Tallinn University of Technology
Tallinn, Estonia
jelizaveta.vakarjuk@cyber.ee

Nikita Snetkov
Cybernetica AS
Tallinn University of Technology
Tallinn, Estonia
nikita.snetkov@cyber.ee

Abstract

Post-quantum cryptography has gained more and more attention with the recent developments in quantum technology. There are already standard drafts for the novel post-quantum cryptosystems and organisations are starting the process of migration to post-quantum cryptography. However, the migration process has many challenges that need to be taken into account. Moreover, the algorithms themselves have become more complicated, making it more difficult to educate people about post-quantum cryptography. We propose to use gamification to make it easier to explain the main challenges and obstacles as well as the main steps of the migration process to the non-cryptographic community. We propose a board game that is built using the gamification taxonomy of Toda et al. to ensure a smooth learning process.

1 Introduction

There are big changes coming to the cryptography world with the new standards of post-quantum cryptography (PQC). PQC refers to cryptographic schemes that work on classical computers, but are resistant to both classical and quantum computer attacks (Alagic et al., 2022). An exact estimation of time when a large enough quantum computer will be available is considered an ambiguous task. However, we can use results from the survey conducted by evolutionQ Inc. (Michele Mosca, 2023), where 37 international quantum computing experts were asked a series of questions about the developments in the field. One of the questions was to identify the likelihood of having a quantum computer that can factorize a 2048-bit number in less than 24 hours in upcoming decades. A majority (20/37) of the respondents answered that it is about 50% likely or more likely to have such quantum computer in next 15 years. Organisations should start thinking of their migration strategies to make the process of switching systems from one class of cryptographic schemes to the other more smooth (Attema et al., 2023). However, with new algorithms, new challenges appear. The fact that new algorithms are more complicated to understand and have different limitations that make it challenging to fit PQC into existing protocols, is among the most prominent challenges. Additionally, the migration process is expected to be more challenging and resource-consuming compared to migration from DES to AES or from SHA1 to SHA2 (Banerjee et al., 2023). Therefore, the challenges that might be encountered during the process are novel and might be unique to each system. Considering increased complexity of the algorithms and challenges, it has become more difficult to educate people on this topic. In this paper, we propose to use gamification to explain the main challenges and steps in the migration process to people with different knowledge backgrounds. We develop a board game, where throughout the game process, players learn different families of PQC algorithms, the main obstacles in the PQC research process and the process of migrating to PQC, how the research process works in general.

1.1 Gamification

Active learning strategies are widely employed in learning environments to better engage learners with the course material, encourage critical thinking and discussions. Studies show that the learners' examination grades improve and the course failure rate decreases, if some of the active learning techniques are used throughout the course (Freeman et al., 2014). One of the examples of active learning is usage of gamification within the educational environment. Gamification has been extensively used for education with

the goal to increase learners' motivation and engagement with the material (Dichev and Dicheva, 2017). It is a supporting mechanism that incorporates various game elements to the educational activities. To add more formalism to the gamification methodology, a gamification taxonomy was proposed by Toda et al. (Toda et al., 2019). The aim of the taxonomy is to support the design of learning environments that are using gamification elements. The taxonomy is split into five dimensions – performance/measurement, ecological, social, personal, fictional. Each of the dimensions has various elements with examples on how those can be implemented in the educational environment. The *measurement dimension* is important for providing learners with feedback on their progress and actions that have been taken during the course of the game. The *ecological dimension* is responsible for the learner's interaction with the game environment. The *social dimension* is connected with the social side of interactions with the environment and the other learners. The *personal dimension* is related to the learner using the game environment. The *fictional dimension* is related to the learner's experience when interacting with the game though narrative and storytelling.

2 Post-quantum trails game

Post-quantum trails is a competitive game, where all the players have the same goal to achieve. The goal of the players is to finish their migration process before the quantum computer is built. Player, who finishes their migration process first, wins the game. If the quantum computer is built before one of the players finished their migration, the game wins. Throughout the game, players are not only focusing on the research actives, but also spend resources on marketing to advertise their research. There are several types of cards in the game – event cards, action cards, and team member cards. Example cards are presented on Figure 1. All the example cards contain pictures generated by the Adobe Firefly [1]. *Event cards* correspond to the main events that are happening in the world and that lead to some consequences in the research process. *Action cards* correspond to the activities that support the research, development and marketing processes. *Team member cards* correspond to the team members that can be hired to move the research and development process forward and improve it.

During the game, players can gain different resources – science points, influence points and money. Science points are needed to advance with research activities, influence points are connected to marketing activities and money is needed to hire new team members and be able to respond to the events coming from the event cards. Some of the event cards speed up the development of the quantum computer.

Event cards The research process can be influenced by different events happening in the field, findings by other research teams and difficulties in funding. For the event cards, we have collected different events from the sources like pqforum, PQC conferences (NIST, PKI, ETSI), Twitter threads of researchers from the field of PQC, papers connected with PQC. The main idea behind these cards is to illustrate what are the challenges of the research process in novel areas, how unexpected findings can destroy some of the development strategies of players, and simulate consequences of some bad events. Event cards contain news that influence their actions for this turn. Additionally, there are cards connected to the development of quantum computing, which are adding quantum tokens to the timeline.

Action cards There are different activities that can support the research process financially and also offer moral support. The content of the action cards is mostly based on the authors' research experience in the field of cryptography. The goal of these cards is to illustrate positive events that occur in the research process. Action cards help players to gain resources and hire new team members.

Migration path On the migration path, the players need to advance their player figures. To advance to the next level, players need to satisfy certain requirements or spend resources. It is possible to skip some of the levels, but if the player decides to complete an optional level it gives them protection against certain events from the event deck. The migration path has the following steps:

1. Security proof (optional) – gives additional science points to the player.
2. Publication – research should be submitted to journals/conferences to be evaluated by the other experts in this area. This step aims to

[1] `https://www.adobe.com/products/firefly.html`

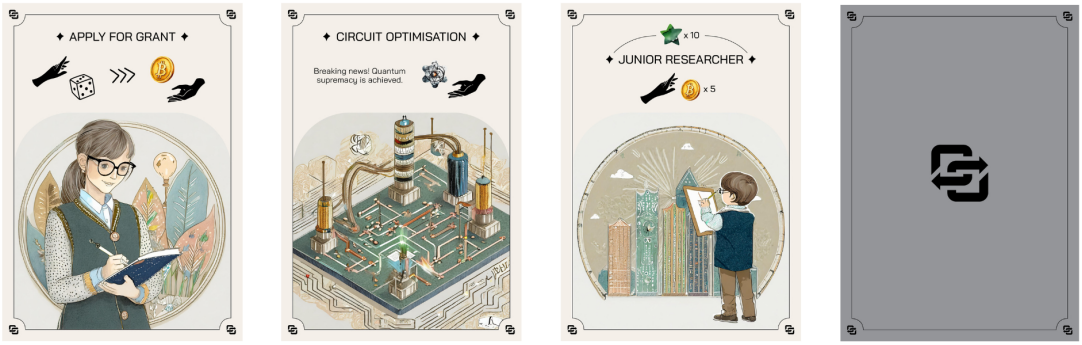

Figure 1: Examples of cards of different type

simulate that before standardisation process researched scheme undergoes initial cryptanalysis.

3. Standard – step inspired by the NIST PQC standardisation process.
4. Hybrid mode (optional) – to make sure that the system is secure even if a novel attack appears on an implemented PQC scheme, it is advised by many organisations (ANSSI, 2023; BSI, 2023; H, 2023) to use PQC together with classical cryptography.
5. Real-life implementation – once the scheme is analysed and selected to be one of the future standards, it should be tested within the real systems. It is essential to perform testing and analysis as early as possible to be able to spot challenges and limitation at early stages and have enough time to fix them.
6. Worldwide usage – this is the final card of the migration path that the player should complete to win the game. It illustrates that the scheme was adopted and is being actively used.

Team member cards In order to be more successful in research and marketing activities, players can hire new team members. There are two main types of team members – researchers and marketing specialists. Researchers award players science points and there are three types of researchers – junior researcher, researcher and senior researcher. Marketing specialist awards influence points that are required to complete the final step of the migration process (worldwide usage).

2.1 Game development

To develop a board game idea and all the game elements that would supplement education process, we used the gamification taxonomy of Toda et al. (Toda et al., 2019). From the measurement dimension, we applied progression, points and stats. *Progression* – during the game, players advance in their migration process which helps them to identify how they move forward to the end goal (building last worldwide usage card of the migration process) Additionally, there is a quantum computer development progression bar, which indicates the approximate time remaining for completing the goal. *Points* – players gain science points and influence points for successfully performing different actions. *Stats* are connected with the progression, when a player moves their figure on the migration path and that shows which tasks the player has successfully completed. All the measurement dimension elements ensure that the players get enough feedback on their progress throughout the game and the game does not end unexpectedly for the players. Therefore, making sure that the players do not get frustrated or disoriented (Toda et al., 2019).

From the ecological dimension, we applied chance, imposed choice, economy, rarity and time pressure. *Chance* is used in different places throughout the game. There are action cards that allow players to gain resources, where the amount depends on the dice roll. There are event cards that are randomly drawn at the beginning of a player's turn that result in different consequences. Finally, players draw action cards at random from the corresponding deck. *Imposed choice* – there are certain migration steps that are not necessary for the successful completion of the end goal, but which bring additional points or provide protection against certain event cards. Players can choose whether to complete these steps or not,

which in turn, influences how the players will advance in the future. *Economy* is directly connected to resources that the players gain during the game. Players are spending gained resources to hire new team members and to participate in the research activities. *Rarity* – there is a limited number cards that give more resources to the players. *Time pressure* – there is the quantum computer development timeline that has a limited number of places that are filled with tokens during the game. Once all the fields are covered by tokens, the game ends. The presence of these ecological dimension elements ensures that the player does not get the feeling that their actions are aimless and do not impact the outcome of the game. Players are presented with the choice over the course of the game, limited resources of certain cards ensure that there will be enough interest among the players to find those rare cards. The addition of some chance elements makes it more interactive and interesting, but the amount of cards related to a random dice roll is limited to mitigate frustration of the players from bad luck and lessen the randomness.

From the social dimension, we used competition and social pressure. *Competition* is present since the players are competing among each other to finish their migration process first and win the game. *Social pressure* is partially achieved through the event deck. Even though, the events are appearing randomly, blame for the events with bad consequences (e.g., adding a quantum token) is put not on the deck itself but on the player who has drawn this card. Through the usage of the social dimension elements, we ensure that the players are motivated by trying to overcome their co-players and accomplish the goal faster. However, some players may be discouraged if they are not doing so well as their co-players. Therefore, our future plans include introducing a cooperative mode where the players will be competing with the game and not with the other players. Another option is to divide players into teams, so they will be competing in teams, not individually, which is less discouraging.

For the personal dimension, we have added the following elements – novelty, objectives, renovation. To achieve *novelty*, we added variability to all the card decks, so there will be enough different events and actions to keep the players engaged. *Objectives* – players have the same end goal, i.e., to complete the migration process. Additionally, there are smaller objectives along the path, for example, to publish a paper in a journal or a conference, a player needs to collect a certain number of science points. *Renovation* – there is a limited number of action cards that can be played together with the other action cards that require rolling a die to decide the outcome. Those cards allow the player to re-roll a die if the initial outcome is not satisfactory for the player. These personal dimension elements ensure that the players are not misguided throughout the game and have a clear goal to accomplish, variability of the cards ensures that the players do not lose interest during the game. Additionally, the renovation element allows players to re-do their unsuccessful actions.

From the fictional dimension, we added the *narrative element*. This is achieved through the introduction to the game, where the players will receive an explanation of the game world and the players' role in this world. Moreover, players draw event cards that are drawn each turn, add details to the game flow that may influence the player's actions during their turn.

3 Future work

The next phase of the research work is to try out the game with different audiences to collect their feedback and improve, clarify and modify the game where needed. Additionally, using the players' feedback, we will analyse if their understanding of the PQC migration process has improved after playing the game. If the players' feedback confirms our concerns about the single-player competitive mode, we will additionally develop a cooperative mode for the game to ensure that the educational environment is not discouraging or frustrating to the learners.

Acknowledgments

This work was funded by the Estonian Research Council under the grant number PRG1780 and the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone. 2022. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8413-upd1, Jul.

ANSSI. 2023. ANSSI views on the Post-Quantum Cryptography transition (2023 follow up). https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography, Aug.

Thomas Attema, João Diogo Duarte, Vincent Dunning, Matthieu Lequesne, Ward van der Schoot, and Marc Stevens. 2023. The PQC Migration Handbook. GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY. Technical report, Applied Cryptography and Quantum Algorithms (TNO) and Cryptology Group (CWI) and Netherlands National Communications Security Agency (AIVD).

Aritra Banerjee, Tirumaleswar Reddy.K, Dimitrios Schoinianakis, and Tim Hollebeek. 2023. Post-Quantum Cryptography for Engineers. Internet-Draft draft-ietf-pquip-pqc-engineers-02, Internet Engineering Task Force, October. Work in Progress.

BSI. 2023. Cryptographic Mechanisms: Recommendations and Key Lengths, Jan. BSI – Technical Guideline TR-02102-1, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html.

Christo Dichev and Darina Dicheva. 2017. Gamifying education: what is known, what is believed and what remains uncertain: a critical review. *International Journal of Educational Technology in Higher Education*, 14(1):9, February.

Scott Freeman, Sarah L. Eddy, Miles McDonough, Michelle K. Smith, Nnadozie Okoroafor, Hannah Jordt, and Mary Pat Wenderoth. 2014. Active learning increases student performance in science, engineering, and mathematics. *Proceedings of the National Academy of Sciences*, 111(23):8410–8415.

John H. 2023. Migrating to post-quantum cryptography, Nov. National Cyber Security Centre blog post, https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc.

Marco Piani Michele Mosca. 2023. Quantum Threat Timeline Report 2022. https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/, December. Accessed: 2023-11-28.

Armando M Toda, Ana C T Klock, Wilk Oliveira, Paula T Palomino, Luiz Rodrigues, Lei Shi, Ig Bittencourt, Isabela Gasparini, Seiji Isotani, and Alexandra I Cristea. 2019. Analysing gamification elements in educational environments using an existing gamification taxonomy. *Smart Learning Environments*, 6(1):16, December.