Shuffle, Cut, and Learn: Crypto Go, a Card Game for Teaching Cryptography

Ana I. González-Tablas [1], **María I. González Vasco** [2,*], **Ignacio Cascos** [3] **and Álvaro Planet Palomino** [1]

1   Computer Science and Engineering Department, Universidad Carlos III de Madrid,
     Avda. de la Universidad, 30, 28911 Leganés, Spain; aigonzal@inf.uc3m.es (A.I.G.-T.);
     aplanet@pa.uc3m.es (Á.P.P.)
2   Department of Applied Mathematics, Materials Science and Engineering and Electronic Technology,
     Universidad Rey Juan Carlos, Calle Tulipán S/N, 28933 Móstoles, Spain
3   Department of Statistics and UC3M-Santander IBiDat, Universidad Carlos III de Madrid,
     Avda. de la Universidad, 30, 28911 Leganés, Spain; ignacio.cascos@uc3m.es
*   Correspondence: mariaisabel.vasco@urjc.es

check for
updates

Abstract: Cryptography is the mathematical core of information security. It serves both as a source of hard computational problems and as precise language allowing for the formalization of sound security models. While dealing with the mathematical foundations of cybersecurity is only possible in specialized courses (tertiary level and beyond), it is essential to promote the role of mathematics in this field at early educational stages. With this in mind, we introduce Crypto Go, a physical card game that may be used both as a dissemination and as an educational tool. The game is carefully devised in order to entertain and stimulate players, while boosting their understanding on how basic cryptographic tools work and interplay. To get a preliminary assessment of our design, we collected data from a series of test workshops, which engaged over two hundred players from different ages and educational backgrounds. This basic evaluation indeed confirms that Crypto Go significantly improves students' motivation and has a positive impact in their perception and understanding of the field.

1. Introduction

Cryptography is the basic science behind the design of secure computation and communication systems. While both industry and academia surely link this area with different fields in mathematics (e.g., number theory, geometry and computer algebra) the starring role of mathematics in this field is hardly disseminated to the general public. In particular, young students have very few opportunities to actually get a glimpse of cryptographic thinking, and far less to connect this discipline with the kind of math they learn at school.

This work presents a card came, Crypto Go, which we designed to help students acquiring and/or reinforcing basic concepts within so-called symmetric cryptography (cryptography without a priori shared secrets). We pursued the design of a training tool suited for a wide audience, from the general public with hardly any prior knowledge to security professionals—who are not always schooled in up-to-date cryptographic developments. To this aim, we believe that the game is indeed most useful if introduced in the context of a specially designed workshop, which may be adapted to the audience in order to:

(a)　show the high-level mathematical ideas behind cryptographic tools and the use in daily life of these tools

　　　a.1.　(target audience: young students) improving how they perceive the importance of mathematics in their studies and lives,

　　　a.2.　(target audience: general public) showing them the relevance of mathematical innovation in information technologies;

(b)　motivate learners to get deeper training in the mathematics of cryptography and, as a consequence, grow the talent pool into the cybersecurity industry needed for the 21st century

　　　b.1.　(target audience: pre-college students, undergraduate students) attracting them to courses and training programs related to mathematics and computing,

　　　b.2.　(target audience: professionals) broadcasting the added value of lifetime learning in the context of mathematical techniques related to information security.

Indeed, fostering curiosity and interest in cybersecurity topics is a challenge, in particular when the target audience is very young and/or lacking mathematics and computing literacy. In this context, game based learning has proven to be a useful resource (see, for instance, the insightful survey [1]). However, it is remarkable that most of the existing cybersecurity games for youngsters focus mainly on security threats and defences in computer networks and, only recently, also include topics related to social engineering and privacy protection. Still, none of these games focuses on modern cryptography, although some make meager use of classical ciphers. We believe that cryptography provides an exceptional context to raise awareness of very important security concepts (i.e., confidentiality, integrity and authentication) and the consequences of not assuring them. In addition, basic cryptographic training can make young students aware of the diverse and variable nature of mechanisms ultimately involved in the design of a secure system, and of how mathematical formalism is vital for describing, analyzing and validating these designs.

1.1. Related Work

Researchers from different disciplines are devoting increasing attention to gamification and serious games as effective instruments for the achievement of individual or corporate goals. One of the contexts where gamification and serious games are used for non-entertainment reasons is education. Notably, the recent review on the topic in [2] shows that half of the research works published in the time period March 2009–February 2014 focused on educational games while the other half focused on entertainment games. On the other hand, there is an increasing need to build a rigorous research framework to test how gamification may benefit non-gaming applications and the reasons behind it, as discussed in [3].

Focusing on cybersecurity, serious games are perceived as useful training tools for several reasons. Indeed, cybersecurity students and professionals are typically attracted to (mainly on-line) games, so playing is a natural engaging method in training programs. Moreover, the technical skills cybersecurity experts typically exhibit are frequently tested through competitions (hackatons/Capture The Flag (typically referred to using the acronym CTF: online competitions where participants look for "flags" that are hidden somewhere in a system). As a result, many serious games have been designed in this context. We conceived Crypto Go from the assumption that physical games have a number of advantages versus digital ones; in particular, they have stronger impact in intrinsic motivations, in competition, socializing, closure, and self-expression. There are also evidences that analog games are more diverse, as they hold the potential to allow different voices into design processes [4], while other authors stress their suitability for younger students (see [5]). As Crypto Go is a physical card game, we subsequently name the most relevant physical games and refer the interested readers to the surveys [6,7]:

- Elevation of Privilege (EoP) (see [8]). Card game designed by Microsoft for teaching threat modelling. It was created as an educational tool for developers and architects, to help them understanding different strategies for examining possible threats to software and computer systems. A recent evaluation of this game can be seen in [9].
- Security Requirements Education Game (SREG) (see [10]). Card game conceived to train and educate stakeholders regarding security requirements and possible attacks. The effectiveness of this game has been evaluated empirically by the authors.
- Capture the Flag Unplugged (see [11]). This is an offline competition, targeting players who may not have the technical skills to participate in a typical CTF. This game has been evaluated on a small experiment involving 36 high-school students, yielding promising results.
- Control-Alt-Hack (see [12]). Table top card game, where players behave as white hat hackers in a security consulting company. According to the authors, fun and engaging gameplay are design priorities over educational messages.
- [d0x3d!] (see [13]). Cooperative tabletop game geared towards getting young students interested in computer security. Informally tested by the authors.
- Decisions and Disruptions. Tabletop game involving role-playing and dealing with security in industrial control systems. Intended for professionals, the authors have used it to identified decision patterns, good practices and typical errors in three different cathegories of security experts [14].
- RISKIO (see [15]). Designed for non-technical players, RISKIO is a tabletop game designed to increase cyber security awareness in companies. The authors tested the players usefulness and ease of use perception, finding significant differences on how students and professionals felt about playing RISKIO.

In spite of the abundance of educational proposals involving games or role-playing activities, most of them focus on advanced information security topics or are geared towards security awareness in a broader sense [16]. In particular, we found no design dedicated to teaching symmetric cryptography and the mathematical ideas behind it. Innovative proposals involving dedicated software or digital tools can indeed be found, such as CYPHER [17], an open-access MOOC-style learning platform, some very creative cryptographic escape-the-room challenges [18,19], or different approaches, such as [20], which explores the use of visualization techniques for teaching cryptography. However, we find that these proposals are not easy to adapt for digitally untrained audiences. Other educational resources, such as the Cryptoclub Project (see [21]) nicely involve simple mathematical tools and crypto puzzles for K12 students, while fail to provide up to date insight for audiences engaged in higher education programs. Thus, we were highly motivated to undertake the design of Crypto Go to fill the existing gap for analog educational games related to cryptography which can moreover be adapted to a wide audience.

We developed a first prototype aiming at a flexible tool that could be adapted to serve as an instructional game in a wide variety of environments, and be useful for boosting motivation in individuals with poor (or even non-existent) prior knowledge in the field. After testing the game informally with our own students (enrolled in STEM degrees) and including small variations in the original design, we decided to carry out an exploratory evaluation in order to understand the usefulness of our initial layout in a broader audience. While a deeper evaluation would indeed be convenient to determine the actual value of Crypto Go, we could certainly assess its positive impact in students motivation and engagement.

Paper roadmap: The game Crypto Go is described in Section 2, where we first introduce the deck mechanics and educational goals pursued by our design (Section 2.2) to further explain (Section 2.3) the setup of our preliminary evaluation: research questions posed, workshops' design, and overview of engaged participants. Section 3 summarizes the results of our analysis, while Section 4 concludes this exposition with some final remarks.

2. Materials and Methods

Our game Crypto Go See (www.cryptogogame.com) was conceived as a wide-audience educational tool, to be used not only in cryptography courses for college students or specialized training for professionals, but also targeting a much wider audience (families, professionals not related to IT, undergraduate students in arts, etc.). While we wanted to configure a game that could help students with a solid cryptographic background to cement relevant concepts, we also pursued a design that could appeal, entertain and, ultimately, get the general public interested in modern cryptography.

2.1. Playing the Game in Context: The Introductory Talk

Our workshops are preceded by an informal introductory talk, where we explain the game dynamics and the main concepts and cryptographic tools involved. In our exposition, we try to bring out related mathematical concepts with which the audience is familiar. For example, when we explain hash functions to undergraduate students (typically, enrolled in engineering degrees), we stress the fact that they are highly non-injective objects (as functions defined in an infinite domain which however range on a set of short bit strings). In addition, we link the concept of key-size for encryption schemes with the notion of convergence they have learnt in basic calculus, remarking that security theorems are essentially of asymptotic nature. As a result, they learn that for "small" keys, many schemes are insecure, while increasing sufficiently the key sizes security is achieved. Here, what sufficiently means depends on the speed of convergence, as they often realize themselves. For younger (K12) students, we typically restrict to informal comments about the different operations involved in symmetric encryption (which either "shuffles" the letters in the cleartext or substitutes symbols according to a certain rule). For instance, at this point we sometimes introduce some simple counting arguments so that they can compute how many ciphertexts may come out from a plaintext word using a prescribed method.

After this introductory talk, learners have not only grasped the game mechanics but, most importantly, they get a glimpse into the mathematical essence behind the tools represented by the different card types.

2.2. The Game

Crypto Go is a card drafting game, where players aim at collecting certain special winning sets of cards, that actually represent solid cryptographic constructions. Decks consist of 108 cards, each of them displaying a concrete modern cryptographic tool. There are six different types of cryptographic tools involved in the game: stream ciphers (SCs), block ciphers (BCs), hash functions (Hs), operation modes (OMs), authenticated encryption modes (AEs), and message authentication codes (MACs). Colors reveal the tool type represented by a card (red for SC, pink for BC, orange for H, yellow for OM, green for AE, and blue for MAC). Each specific card will thus show the name of a particular tool (such as the block cipher AES or the hash function MD5), followed by a short note with related information (see Figure 1).

In addition, players are given two cheat cards which explain how these tools interplay in order to derive a secure cryptographic construction (in some sense).

In addition, a simple encoding is sketched in the cheat cards: $\sqrt{}$ for secure tools, $\sim$ for those likely to remain secure in the next 5–10 years and $\times$ for tools that are known to have severe security problems—and should be avoided. These cheat cards are an extremely simplified summary of the security recommendations contained in the ECRYPT CSA report [22]. (We actually include a disclaimer in the game instructions emphasizing that the game rules should by no means be used for guiding real-life implementations or developments).

Figure 1. Crypto Go: card sample for each tool type and cheat cards.

2.2.1. How to Play

The goal of each player is to form as many Crypto Kits as possible; a Crypto Kit is a card set representing cryptographic tools that suffice to attain the three main qualities targeted in symmetric cryptography: confidentiality, integrity, and authentication (typically represented by the acronym CIA).

Figure 2 shows the card combinations yielding valid Crypto Kits. For instance, a Crypto Kit can consist of an SC card, a MAC card, and either a BC or an H card.
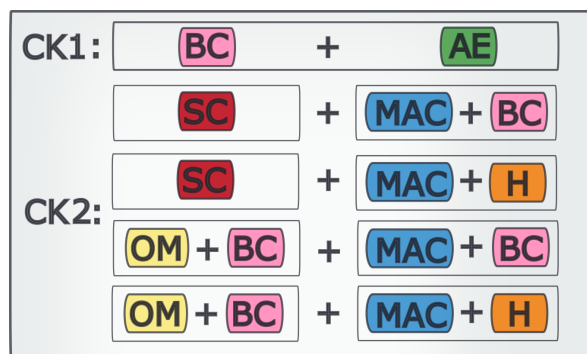

Figure 2. Summary of Crypto Kits.

The game mechanics are as follows: first, cards are shuffled and each player is given six cards, leaving the rest upside down on a main deck in the centre. Now each player chooses a card from her hand and leaves it on the table, upside down. When all players have done this, everyone reveals her chosen card by turning it face-up. Next, each player passes her hand to her neighbour on the left. Thus, in the next turn, everyone has a new hand containing one card less. The procedure is repeated until the hand received by each player contains only one card. At this moment, a special turn begins at which each player takes four cards from the main deck, and from the five cards he/she now holds, each player must choose and play a card (as in a normal turn). Furthermore, each player may use the cards in his/her hand to replace up to two of his/her already played cards, discarding the cards that have been substituted in a face-down pile on the table. Now, before passing hands once more, each player should take from the main deck as many cards as he/she has substituted (so that anyway a hand of four cards is passed). Now, the game direction shifts and normal turns are played until everyone is empty handed.

When there are no cards left to pass and each player has collected 10 cards, the round ends and scores are publicly computed. Players score 16 points for each completed Crypto Kit. However, poor security properties have a price: 2 points must be subtracted for every involved card with medium security level, and 4 points for every card with low security level. On the other hand, for each Crypto Kit constructed only with high security level cards, 4 extra points are awarded (i.e., 20 points are scored for a pristine Crypto Kit). See learners playing Crypto Go in Figure 3 bellow.

Figure 3. Learners playing Crypto Go.

The player with the highest score after three rounds wins the game. Note than Crypto Go decks contain unequal numbers of cryptographic cards of each given type. Each such number depends on how frequently the card is used for building Crypto Kits. For instance, BC cards can be used in up to five different Crypto Kit constructions; as a result, there will be many BC cards in a deck. However, AE cards are (for the same reason) scarce. Being aware of the card type distribution is critical for developing the best winning strategy. Moreover, remembering which tools are useful for deriving secure constructions is a big plus for mastering the game.

2.2.2. Educational Goals Behind Our Design

Our main inspiration behind the design of Crypto Go is the card game Sushi Go (See https://gamewright.com/product/Sushi-Go) for more information about Sushi Go game. This is a highly popular entertainment card game, which can be played and enjoyed even by very young kids. On the other hand, Crypto Go rules and mechanics have been carefully designed to help students automatize the choice and discrimination of cryptographic tools. This ability is really valuable nowadays, as, for instance, obsolete cryptography is often used in certificates which, however, are not identified as invalid by some web browsers.

Moreover, we wanted to help students telling apart the three CIA elements, and gaining a basic understanding of how they are obtained from (often familiar) mathematical tools. Informally, confidentiality is attained if only legitimate recipients have access to the message contents, typically through encryption methods that involve some masking operation with a secret element in a prescribed algebraic structure. In turn, integrity provides non-tampering assurance to the authorized recipient. Further, authentication is achieved if a message source can be validated. These last two goals are typically achieved using tagging functions which allow for the construction of mathematical evidences of origin and intactness. A high level explanation of how these functions work can be given using basic concepts from high-school mathematics (function range and domain, injectivity, preimage, etc.).

While these three CIA properties are closely related, it is important to understand that they are distinct and cannot always be achieved using the same cryptographic tools. Each Crypto Kit is a card assortment representing a set of cryptographic tools that suffice for achieving (in a simplified setting) these three pillars of secure communication. Collecting cards that at the end of the game will fail to guarantee all three CIA qualities is a bad strategy when playing Crypto Go, just as it is in cryptographic practise. On top of this, the game mechanics are carefully pondered so that frequent playing will help students in many different aspects:

- Remembering the names of insecure primitives. Indeed, getting rid of cards representing weak cryptographic primitives is one of the key points of a winning strategy, so the faster a player identifies penalizing cards, the better!

- Identifying which cryptographic tools may be combined. Again, a clever organization of the kept cards results in a higher final punctuation. The special turn is designed to favor players who are agile in this respect.

- Realizing the usefulness of authenticated encryption. The green cards, representing tools for authenticated encryption (AE), are required for short (2-card) Crypto Kits. Thus, they are the main object of desire for players, who quickly grasp the value of these cryptographic tools (which are relatively new and often overlooked in basic cryptography courses).

- Understanding the relevance of key sizes and hash-function ranges. A frequent mistake that students make when they first approach symmetric cryptography is not paying enough attention to parameters. Indeed, as parameters are typically adjusted considering the asymptotic behaviour of certain functions arising in security proofs, it is important to send the message that concrete figures do make a difference. (This is also a great real-world example showing the impact of convergence speed to students knowing basic calculus.) Novel practitioners "tag" a hash function (say SHA-2) as secure or insecure, forgetting that size matters: i.e., the output size is crucial to determine the security level (see the cheat cards in Figure 1). Several cards in Crypto Go represent tools for which reading carefully the number besides the name indeed makes a difference.

Finally, special care has been taken in using color to help learners telling apart different cryptographic tools (and also for achieving a visually appealing design).

2.3. Initial Evaluation of Crypto Go

We have pursued an initial evaluation of Crypto Go, trying to assess its impact on the learning process. Our goal was not only to make improvements in subsequent versions of the game, but also to adapt its usage in order to get the best possible results when interacting with different audiences. For this purpose, we collected data from several workshops involving over 200 participants.

2.3.1. Research Questions

We focused on three research questions in order to understand to what extent learners would perceive our design as attractive and useful for learning. Furthermore, we explored whether gender or game-proneness played a role in the effectiveness of Crypto Go.

Hypothesis 1 (H1). *Learners perceive Crypto Go as a high quality educational game. Before assessing the impact of the game on learners, it is critical to measure the game's educational quality, as this can notably influence the results. As we were pretty certain about the game's playability, appealing design and relation to targeted learning outcomes (see Section 2.2.2), our expectations were that learners would evaluate Crypto Go as an educational game of significant quality.*

Hypothesis 2 (H2). *Learners perceive Crypto Go as an educational asset of significantly higher quality than a non game-based equivalent task. More precisely, we want to establish whether Crypto Go has a significantly higher positive effect on motivation, user experience and perceived learning than a non game-based substituting task. We expected this to be the case, as it is stated in [2] that there is significant evidence in the literature on the increased reactions regarding effective outcomes produced by games used in educational contexts.*

Hypothesis 3 (H3). *The effectiveness of Crypto Go is influenced by gender and/or gaming frequency. Following [3], we find it relevant to explore different factors that may influence the effectiveness of our game. In this work, we restricted our study to game-proneness and gender.*

2.3.2. Workshops

Our research was conducted through several workshops, which included an introductory talk presenting the targeted knowledge concepts, followed by a reinforcing activity. We consider two types of reinforcing activities: one game-based, using Crypto Go, and another one non game-based, using a substituting activity, for control workshops.

In the introductory talk, we explained the targeted mathematical and cryptographic concepts with the support of colorful slides and manipulatives, adapting the tone and contents to the workshop participants (the younger and less experienced, the more informal the tone and the less fine-grained the exposition of concepts). Before explaining the targeted concepts, we established that the context of the whole workshop was communication through the Internet (e.g., accessing some popular video sharing service or social network). This is an activity that most people perform daily and focusing the workshop around this type of communication and its security helps participants link the workshop concepts with previous knowledge and experience.

In game-based workshops, the introductory talk was followed by a description of Crypto Go elements (highlighting how they represented concepts introduced in the talk) and its mechanics. We refer the reader to Section 2 for a thorough description of Crypto Go. Afterwards, participants were organized in groups of 4 to 6 players around a table to play at least two rounds of Crypto Go.

In control workshops, the Crypto Go experience was replaced by a substituting activity that was designed to imitate as much as possible the mechanics of the game, except for the gaming characteristics (social competition, scores, appealing design, etc.). Specifically, this activity consisted of two paper-based exercises in which learners were given a list of 16 cryptographic constructions (together with their tool type and security level), and they had to select 10 of them to build as many combinations achieving the three CIA, with the highest possible security. Participants were then asked to organize in pairs and were given some time to provide an answer to the two exercises. Afterwards, a possible solution for each exercise was shown and discussed with the whole group of learners. In order to evaluate the quality of Crypto Go as an educational game we have used the questionnaire proposed in the MEGAA model described in [23], that follows a post-test design. We used the version for non-digital games and made minor modifications. An exposition in English of the main ideas in [23] (which is written in Portuguese) can be found in [24,25]. From the the questionnaire defined in MEGAA, we have derived a normalized score of the quality of an educational game as the sum of the values given by a learner for each of the items in the questionnaire, normalized over a $[0, 1]$ range. We have also derived a normalized score for each of the factors composing the MEGAA model (motivation, user experience, perceived learning), in order to facilitate comparisons.

In order to compare results between game-based and control workshops, we have adapted MEGAA's items to assess the same factors but referring to a (substituting) activity instead of a game. For example, if the original item in the MEGAA questionnaire read as "I would like to play this game again", we rephrased it as "I would like to do this activity again".

A total of 11 workshops were arranged, belonging to two different types: three within formal STEM dissemination events (most of them for either general public or K12 students) and eight with several local education institutions (high schools, colleges, and universities). The workshops took place from November 2018 till February 2019. In the case of workshops with experienced participants, we searched specific settings and decided to conduct a game or a control treatment seeking to balance the numbers of participants receiving each treatment. All workshops involving non-experienced participants were game-based and concepts were introduced in a more informal way (see Figure 4).

(**a**) One of the researchers at Madrid Science Fair 2019

(**b**) Manipulatives for informal workshops

Figure 4. Workshops.

2.3.3. Participants

In total, we collected data from 223 participants. We divided them in three age groups: 14–18 (where we had 75 participants), 19–21 (to which 120 participants belonged) and 22–28, where we had 28 learners joining in. With respect to gender, we had 54 females and 164 males, while five participants did not declare their gender (see Figure 5b). Out of the 223 participants, 163 of them played Crypto Go, while the other 60 comprise the control group. As expected, the majority of the younger participants (14–18 years old) had no previous experience in cryptography, so most of them attended a Crypto Go (game-based) workshop. In the other two age groups roughly 40% of the participants were assigned to a control workshop: 48 from the first group (ages 19 to 21) and 11 from the 22–28 years old group (see Figure 5a).
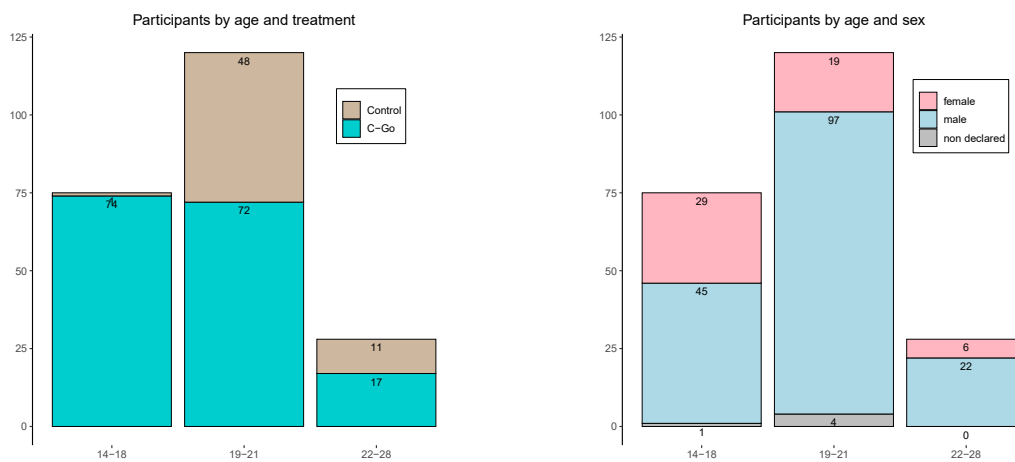
(**a**) By age and treatment

(**b**) By age and sex

Figure 5. Participants.

3. Results

We have used the statistical software R for the analysis below.

3.1. MEGAA: Results (H1, H2)

A first natural goal is to evidence the game's quality. For that purpose, we follow several authors in using a variable MEGAA to aggregate the scores of the three involved variables: motivation, user experience, and perceived learning. In Figure 6 we present boxplots of the MEGAA score, and scores for factors motivation, user experience, and perceived learning, with individuals grouped as those who played Crypto Go (C-Go) and as those who did not (control group).
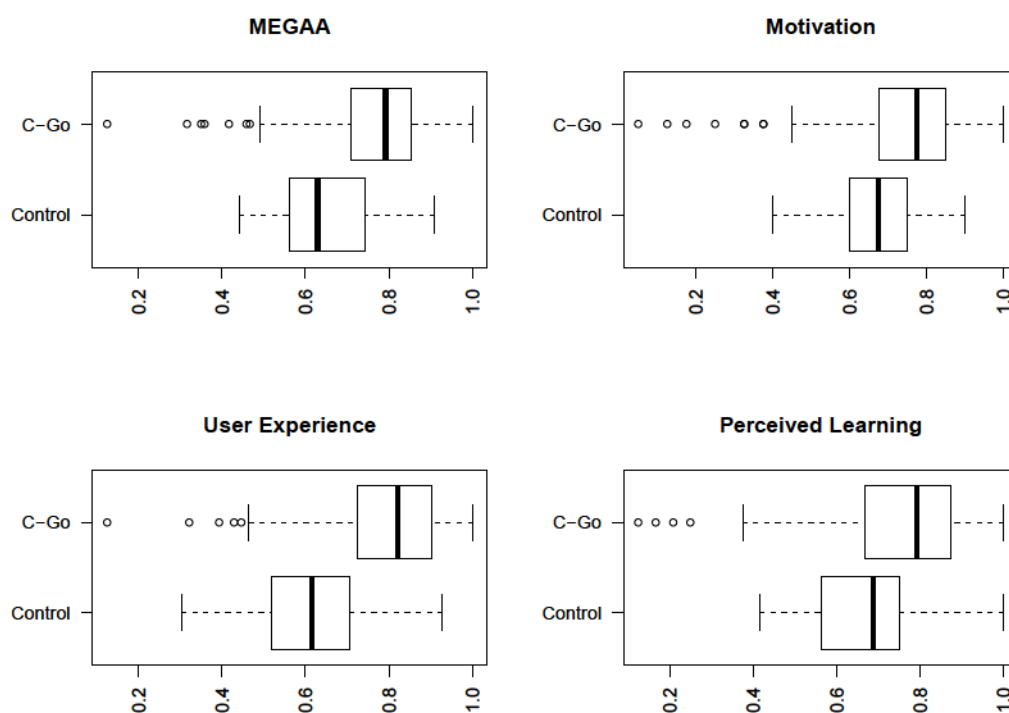
Figure 6. MEGAA results.

The results displayed in Figure 6 suggest that our research hypotheses H1 and H2 were satisfied. Indeed, the unpaired two-samples Wilcoxon–Mann–Whiney one-sided test confirms that there was a positive shift in the MEGAA distribution when Crypto Go players were compared with the control group (approximate p-value 1.5×10^{-10}). In fact, such a positive shift arose in all MEGAA's constituent factors, being more apparent in the variable user experience, whose p-value was almost negligible, but it is still below 10^{-5} in motivation and perceived learning. Figure 6 also shows that the variability of every considered variable on Crypto Go players was greater than in the control group, which happened because the group of Crypto Go players was more heterogeneous than the control one.

3.2. MEGAA: Testing Influence of Gender/Game-Proneness (H3)

In order to have a sample with similar representation of both genders and a wide variety of gaming frequencies, we restricted the study to participants with ages ranging from 14 to 18 years old, who had no previous experience with cryptography. In this group we collected game-proneness data from 61 individuals (35 boys and 26 girls), two of whom declared not to play games at all, 29 to be occasional players, and 30 to play games often.

In our experimental study, females seemed to obtain higher MEGAA scores than males, nevertheless this was highly influenced by three male students with very low MEGAA scores which could be considered as outliers. After their deletion, the average MEGAA score of the females was still slightly greater than the one of the male students, but their difference was not statistically significant. After running normality tests and comparing their variances and means, both samples can be assumed to have been taken from the same normal population.

On the other hand, when comparing regular versus occasional players, we could not find significant differences in their MEGAA scores, and again both samples can be assumed to have been taken from the same normal population.

4. Conclusions

We have presented an educational card game, Crypto Go, and an initial evaluation of it. Using the well-stablished MEGAA model, we evidenced that our game improves on traditional teaching methods in different aspects. More precisely, the results obtained in the previous section can be summarized in the following points:

- Crypto Go shows positive results, outperforming a (traditional) educational activity, in all parameters tested in MEGAA (motivation, user experience, perceived learning).
- Neither gender, nor game-proneness seem to influence the Crypto Go MEGAA scores.

We note that our study is only preliminary, and should indeed be further refined as in our experiments, control groups (engaged in the substituting task) are less heterogeneous since they are always formed by students having a (somewhat solid) background in computing. It is also fair to remark that as the didactic talk was always part of our experiments, we cannot separate its effect from that of the game or substituting task. This does not affect the comparison between the two activities (the talk was given in the same way and by the same researchers in both workshop types), yet it may indeed limit the accuracy of our individual analysis of Crypto Go.

Further, we are convinced that the influence of Crypto Go in objective learning should be explored in order to understand its actual value as a training tool. Based on the informal feedback we got from K12 students and their teachers after our workshops, we believe that our game has a positive influence in fostering motivation and excitement towards mathematics. In addition, older students (undergraduates) often claimed that the workshops made them appreciate the practical value of basic related courses (namely linear algebra and discrete mathematics). It would indeed be very interesting to confirm this impressions through rigorous experiments. In our opinion, these investigations should be carried out on groups of learners who have been playing frequently for a period of at least 3–4 weeks, as it takes time to assimilate both the game mechanics and the mathematical concepts involved.

Conflicts of Interest: The authors declare no conflict of interest.

Ethics Statement: Written consent with our privacy policy was obtained from workshop participants, who were informed in advance of the general aim of the research, its duration, and the procedure to collect, anonymize, store, and analyze their responses to our Crypto Go questionnaires. Our workshops were organized in the context of different events (science fairs, dissemination activities etc.) involving Universidad Carlos III and/or Universidad Rey Juan Carlos, which own the game's copyright.

References

1. Battistella, E.P.; Gresse von Wangenheim, C. Games for Teaching Computing in Higher Education—A Systematic Review. *IEEE Technol. Eng. Educ.* **2016**, *1*, 8–30.
2. Boyle, E.A.; Hainey, T.; Connolly, T.M.; Gray, G.; Earp, J.; Ott, M.; Lim, T.; Ninaus, M.; Ribeiro, C.; Pereira, J. An update to the systematic literature review of empirical evidence of the impacts and outcomes of computer games and serious games. *Comput. Educ.* **2016**, *94*, 178–192. [CrossRef]
3. Treiblmaier, H.; Putz, L.M.; Lowry, P.B. Setting a definition, context, and research agenda for the gamification of non-gaming systems. *AIS Trans. Hum.-Comput. Interact. (THCI)* **2018**, *10*, 129–163. [CrossRef]

4. Troner, E.; Trammell, A.; Waldron, E.L. Reinventing Analog Game Studies. *Analog Game Stud.* **2014**, *1*. [CrossRef]

5. Marchetti, E.; Petersson Brooks, E. Setting Conditions for Learning: Mediated Play and Socio-material Dialogue. In *Design, User Experience, and Usability. Health, Learning, Playing, Cultural, and Cross-Cultural User Experience*; Marcus, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 238–246.

6. Tioh, J.; Mina, M.; Jacobson, D.W. Cyber security training. A survey of serious games in cyber security. In Proceedings of the IEEE Frontiers in Education Conference (FIE), Indianapolis, IN, USA, 18–21 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.

7. Mirkovic, J.; Dark, M.; Du, W.; Vigna, G.; Denning, T. Evaluating Cybersecurity Education Interventions: Three Case Studies. *IEEE Secur. Priv.* **2015**, *13*, 63–69. [CrossRef]

8. Shostack, A. Elevation of Privilege: Drawing Developers into Threat Modeling. In Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), San Diego, CA, USA, 18 August 2014; USENIX: San Diego, CA, USA, 2014.

9. Tøndel, I.A.; Oyetoyan, T.D.; Jaatun, M.G.; Cruzes, D. Understanding Challenges to Adoption of the Microsoft Elevation of Privilege Game. In Proceedings of the HoTSoS'18 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security, Raleigh, NC, USA, 10–11 April 2018; ACM: New York, NY, USA, 2018; pp. 2:1–2:10.

10. Yasin, A.; Liu, L.; Li, T.; Wang, J.; Zowghi, D. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). *Inf. Softw. Technol.* **2018**, *95*, 179–200. [CrossRef]

11. Ford, V.; Siraj, A.; Haynes, A.; Brown, E. Capture the Flag Unplugged: An Offline Cyber Competition. In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education, SIGCSE'17, Seattle, MA, USA, 8–11 March 2017; ACM: New York, NY, USA, 2017; pp. 225–230.

12. Denning, T.; Kohno, T.; Shostack, A. Control-Alt-Hack^TM: A card game for computer security outreach and education (abstract only). In Proceedings of the 44th ACM Technical Symposium on Computer Science Education, SIGCSE '13, Denver, CO, USA, 6–9 March 2013; ACM: New York, NY, USA, 2013.

13. Gondree, M.; Peterson, Z.N. Valuing Security by Getting [d0x3d!]: Experiences with a Network Security Board Game. Presented at the 6th Workshop on Cyber Security Experimentation and Test, Washington, DC, USA, 12 August 2013.

14. Frey, S.; Rashid, A.; Anthonysamy, P.; Pinto-Albuquerque, M.; Naqvi, S.A. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Trans. Softw. Eng.* **2019**, *45*, 521–536. [CrossRef]

15. Hart, S.; Margheri, A.; Paci, F.; Sassone, V. Riskio: A Serious Game for Cyber Security Awareness and Education. *Comput. Secur.* **2020**, *95*, 101827. [CrossRef]

16. Center for Development of Security Excellence. Security Awareness Games. Available online: https://www.cdse.edu/resources/games.html (accessed on 2 November 2020).

17. Younis, A.Y.; Kifayat, K.; Shi, Q.; Matthews, E.; Griffiths, G.; Lambertse, R. Teaching Cryptography Using CYPHER (InteraCtive CrYPtograpHic Protocol TEaching and LeaRning). In Proceedings of the 6th International Conference on Engineering ICEMIS, Almaty, Kazakhstan, 14–16 September 2020; ACM: New York, NY, USA, 2020; pp. 1–7.

18. Deeb, F.A.; Hickey, T.J. Teaching Introductory Cryptography using a 3D Escape-the-Room Game. In Proceedings of the IEEE Frontiers in Education Conference (FIE), Covington, KY, USA, 16–19 October 2019; pp. 1–6.

19. Ho, A. Unlocking Ideas: Using Escape Room Puzzles in a Cryptography Classroom. *PRIMUS* **2018**, *28*, 835–847. [CrossRef]

20. Simms, X.; Chi, H. Enhancing cryptography education via visualization tools. In Proceedings of the 49th Annual Southeast Regional Conference, Kennesaw, GA, USA, 24–26 March 2011; Clincy, V.A., Hoganson, K.E., Garrido, J., Dasigi, V., Eds.; ACM: New York, NY, USA, 2011; pp. 344–345. [CrossRef]

21. CryptoClub Project Team, University of Chicago. CryptoClub Project. Available online: www.cryptoclub.org (accessed on 20 August 2020).

22. Abdalla, M. Document D5.4 Algorithms, Key Size and Protocols. In *ECRYPT – CSA (ICT–2014—Project 645421)*; ECRYPT Project: Bristol, UK, 2018.

23. Savi, R.; von Wangenheim, C.G.; Borgatto, A.F. A model for the evaluation of educational games for teaching software engineering. In Proceedings of the 25th Brazilian Symposium on Software Engineering (SBES), Sao Paulo, Brazil, 28–30 September 2011; pp. 194–203.

24. Petri, G.; von Wangenheim, C.G.; Borgatto, A.F. A large-scale evaluation of a model for the evaluation of games for teaching software engineering. In Proceedings of the IEEE/ACM 39th International Conference on Software Engineering: Software Engineering Education and Training Track (ICSE-SEET), Buenos Aires, Argentina, 20–28 May 2017; pp. 180–189.

25. Petri, G.; von Wangenheim, C.G.; Borgatto, A.F. *MEEGA+: An Evolution of a Model for the Evaluation of Educational Games*; Technical Report; INCoD/GQS: Florianópolis, Brasil, 2016.