

Can We *Formally* Catch Cheating in E-exams?

Itzel Vazquez Sandoval and Gabriele Lenzini^a

Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg

Keywords: Cheating, Secure E-exams, Security Protocols, Socio-technical Analysis, Formalization of Cheating.

Abstract: Cheating in exams is a practice as old as exams themselves. Institutions and examiners have learned to mitigate traditional ways of cheating, such as the use of crib notes. Yet, the massive digitalization of the world has facilitated the application of electronic exams (e-exams), for which more innovative and sophisticated ways of cheating have emerged. The advent of Information and Communication Technology is changing the threat model as the e-exam environment is not restricted to a classroom anymore; and examiners are simply not well-equipped to supervise a digitally connected network. To a large extent, the research on the subject follows one of two main approaches: philosophical, focused on trying to understand the causes and behaviors of cheaters; or pragmatical, aimed at providing means for preventing or detecting fraudulent scenarios. Here, we take a different perspective and look at cheating as a theoretical information security problem. More specifically, we aim at finding specifications that allow us to unequivocally decide whether an examinee has tried to subvert an exam protocol by using unauthorized means to answer questions. We discuss how we could formalize such definitions and comment on different frameworks suitable for the task. Our discussion provides insights into future research directions towards devising formal frameworks for a rigorous study of cheating scenarios and thereby, the development of e-exam systems that would be resilient to such scenarios by design.

1 INTRODUCTION

The Oxford Advanced Learner's Dictionary defines cheating as "to act in a dishonest way in order to gain an advantage, especially in a game, a competition, an exam, etc.". It is not a coincidence that the definition mentions *exams*, because cheating is as old as their existence. Typical practices include obtaining the questions of a test beforehand, copying or getting answers from another student, and using unauthorized crib notes (Bjorklund and Wenestam, 1999).

With the global spread of mobile phones and the affordability of connectivity, students started relying on technology to seek help for solving tests. With the use of digital communication channels, cheating has reached a worrisome level of growth. Books like "La Fabrique de Tricheurs" (Guénard, 2012) report, based on feedback by ministers, teachers, and parents, that Information and Communication Technology (ICT) has transformed cheating from being folklore into a true industry of fraud.


The establishment of online courses and the dissemination of electronic exams (e-exams)—either computer-aided and hybrid, or internet-based—have

simply amplified and worsened the phenomenon.

Cheating has not only increased, but is pursued using innovative techniques, against which the common anti-fraud strategies used in traditional exams—e.g., proctoring—do not work well or at all. Moreover, the prevailing perception among students is that cheating on e-exams is easier than cheating in traditional courses (Søgaard, 2016; Moten Jr et al., 2013; Backman, 2019). The most common method consists of students collaboratively solving an online exam while searching for answers on the Internet or in online course material (Backman, 2019; Li et al., 2021).

The reality is that preparing, deploying and running an exam is a complex endeavour, usually involving several parties organizing, coordinating, and controlling activities. Despite the great efforts put into these tasks, cheating remains common while detection rates are typically low (Bjorklund and Wenestam, 1999). The difficulty of setting up an effective and scalable proctoring process during the execution of e-exams increases the chances of success for cheaters, and lowers the risk of them facing consequences.

In this position paper, we intend to draw attention to the phenomenon of cheating in e-exams, to eventually discuss what instruments could be employed to

^a  <https://orcid.org/0000-0001-8229-3270>

determine whether someone has cheated, what evidence we need for that decision, and whether we can design e-exam protocols that mitigate, discourage, or impede acts of cheating.

Such a long term goal must begin with an understanding of what “cheating” means and of what the threat models are, i.e., the scenarios and the modalities wherein cheating can take place.

We first give an overview of approaches that deal with cheating at different phases of e-exams; then, we focus on cheating at the moment of solving the exam and propose new research directions to study the problem in ways that would inherently provide stronger security guarantees.

Contributions and Structure. After introducing some preliminaries on e-exams in Section 2, the main contributions of this paper are:

- A systematization and classification of prevailing approaches aimed at securing the different phases of an e-exam (Sections 3 and 4); the classification criteria offers a simple way to categorize new research on secure e-exams.
- A few preliminary attempts at providing a formal categorization of cheating during an ongoing e-exam (Section 5).
- Potential research directions to advance the state-of-the-art in formal approaches for the definition, prevention and detection of cheating at examination time (Section 6).

2 PRELIMINARIES: E-EXAMS

The term e-exam typically refers to computer-based or computer-aided systems that enable the assessment of students. Different e-exam systems consider different roles, yet, invariably there are *candidates* or *examinees*, *examiners*, and an *exam authority* who manages the registration, exams, grades and interactions.

According to (Giustolisi et al., 2013), an e-exam is typically organized in four different phases:

Registration. The examination authority creates a new exam and candidates who comply with the eligibility criteria get registered.

Examination. Registered candidates receive a set of questions and then submit their corresponding answers to the examination authority. At the beginning of this phase, the candidates are usually authenticated.

Marking. The examination authority distributes the candidates’ answers among the examiners, who evaluate and mark them.

Notification. Marks are assigned and notified to their respective candidates.

We could identify more explicitly a phase *Preparation*, in which the questions are selected, pre-answered, and printed or prepared to be deployed. In (Giustolisi et al., 2013), this phase is included in *Registration*.

E-exams can be grouped according to the restrictions that they enforce in the environment and in the system; for instance, whether examinees can be physically located anywhere and use their own devices (e.g. exams via Moodle), whether they have to install dedicated software for controlling the resources available (e.g., Safe Exam Browser(SEB) (Schneider et al., 2010)), or if they are asked to be at a designated center and use a provided workstation (e.g. TOEFL iBT).

This classification becomes relevant from a security point of view, for the formal modeling of e-exam systems and for the definition of adversarial models.

3 CHEATING IN E-EXAMS

Cheating in e-exams can be seen as a deviation from the established e-exam protocol, at any of the phases, with the purpose of giving the examinee an advantage over the regular process.

Cheating exposes security vulnerabilities of an e-exam system as it implies a violation of the restrictions imposed on the parties involved in the e-exam. Considering this, here we are concerned with the security of the systems with respect to such adversaries, i.e., examinees, examiners, exam authorities (Section 2). For a given e-exam instance e_i , attacks that affect the e-exam system with a purpose other than cheating in e_i are out of our scope.

To contextualize our focus of study, we provide a classification of cheating techniques depending on the e-exam phase in which they take place.

3.1 Before or after Examination

Adversary: any role (or group of them).

These are attempts at taking advantage of vulnerable steps of the process, prior or posterior to the Examination phase. Taking the exam for someone else in the absence of proper authentication, or collusion of examinees with examiners to get better grades, are examples in this category.

Strategies for mitigating this kind of cheating involve the design of e-exam protocols that are proven and verified to provide certain security properties,

for instance, candidate authentication, collusion resistance, anonymous marking, and marking integrity (Dreier et al., 2014; Dreier et al., 2015). We elaborate further in Section 4.1.

These approaches usually assume that Examination is supervised to ensure that candidates do not cheat at runtime.

3.2 During Examination

Adversary: the examinee (or a group of them). This classification refers to unauthorized methods used during the execution of an e-exam in order to obtain and provide the correct answers to the given set of questions, such as accessing disallowed resources or communication with others.

Practical strategies discussed in the literature to minimize the impact of these methods target the design of e-exams (Sindre and Vegendla, 2015; Moten Jr et al., 2013; Sjøgaard, 2016; Backman, 2019; Li et al., 2021). Suggestions include maximizing the number of questions in a given time, randomizing the order of the questions, revealing the next question only after the previous one has been answered, and creating different types of exams—making use of available pools of questions—each of which should be distributed to a group of examinees with similar competences.

A more sophisticated subset of these cheating techniques attacks the e-exam systems, tampering with the software and/or hardware in place. Examples include running a script to copy the exam questions into the examinee’s device, using a USB key to inject crib notes into the exam environment, or overwriting the controlling software to allow restricted copy-paste functionality (Dawson, 2016). Some of these attacks can be mitigated by surveillance, network restrictions, or blocking the web camera, microphone and audio on the examinee’s computer.

As far as we know, there has been neither any formal studies concerning the robustness of such techniques nor any formal proofs with respect to defined adversarial models.

4 PREVENTION & DETECTION

Math-based solutions that deal with the problem of cheating in e-exams can be classified according to the approach that they take, either for the prevention of cheating, or for its detection once it has happened. Preventive approaches primarily rely on cryptography and formal methods, while detective approaches lean towards statistical analysis and machine learning techniques.

4.1 Preventive Approach

Preventive approaches aim at constructing e-exam systems resilient to cheating behavior from a subset of the involved parties; they largely target the cheating techniques discussed in Section 3.1.

These solutions are mostly based on cryptographic protocols and ceremonies—protocols extended by including the human interactions—for e-exams that are proved to satisfy certain security properties against specific attacker models, hence, guaranteeing that particular cheating scenarios cannot occur. The proofs of security are usually carried out by symbolic analysis of abstract protocol models, looking for potential flaws in the logic of protocol specifications.

In this line of research, (Castella-Roca et al., 2006) proposed a secure e-exam management system where authenticity of questions and examinees’ identity, secrecy of grades and of exam questions are guaranteed; the scheme relies on a Trusted Third Party (TTP) to manage the process, questions, answers, and grades. (Huszi and Petho, 2010) propose a system that provides similar guarantees without relying on a TTP. (Bella et al., 2015) propose a protocol, independent of TTPs too, that provides an extended set of security properties—e.g. the party responsible for a protocol failure can be identified—for which they provide formal proofs of security.

Notably, a common assumption in these schemes is the existence of a supervised examination center or some sort of invigilation in place—e.g. continuous authentication mechanisms, proctor software, trackers—to mitigate illegitimate actions aimed at providing the correct answers during the exam.

The security properties relevant for these protocols aim at preventing the participants from tricking the e-exam process (e.g. *anonymous marking* prevents a student from colluding with an examiner to get a specific grade). An informal classification was given by (Furnell and Karweni, 2001). A fundamental set of security properties relevant for e-exams has been defined and formalized by (Dreier et al., 2014); such properties concern primarily authentication and secrecy. (Dreier et al., 2015) extend this work with so called *verifiability* properties of e-exams; individual verifiability properties allow examinees to check having received the correct marks for their answers, while universal ones allow outsider auditors to verify the correctness of the process, e.g., whether only registered candidates participate in the exam, or that marks are assigned to the corresponding examinees. (Kassem et al., 2015) propose a similar set of properties using a formalization based on events. They mainly ensure that: only registered examinees take

the exam, accepted answers are submitted by examinees, answers are accepted only during the exam duration, and marks are correctly computed and assigned to the corresponding candidates.

As a remark, although the security properties that they verify are similar, the work by (Kassem et al., 2015) differs from the previous ones as it verifies whether cheating took place in a particular e-exam execution, while the others ensure that a cheating scenario cannot occur in any run of an e-exam protocol. We discuss further Kassem’s approach in Section 4.2.

4.2 Detective Approach

Detective approaches aim at post-exam identification of cheating behavior, in particular, the occurrence of forbidden actions during the examination phase that could have led the examinees to providing the correct answers; these solutions deal with the cheating techniques described in Section 3.2.

The vast majority of techniques for the detection of unauthorized runtime cheating (i.e., at the examination) rely on statistical methods over observable factors. Some approaches base their analysis on the wrong answers observed across the exams of a group (DiSario et al., 2009); others (e.g. (Fan et al., 2016; Awad Ahmed et al., 2021) and references therein) analyze the input of eye trackers, or other sensors. (Dsouza and Siegfeldt, 2017) proposed a framework with ascending complexity levels (from graphical data representation to regression analysis) for determining whether cheating has taken place in online or take-home exams.

An increasingly growing area of research makes use of machine learning based techniques for detecting exam frauds. For instance, (Kamalov et al., 2021) propose the training of a recurrent neural network model with scores of quizzes, midterm exams, etc, to predict final exam scores; significant deviations of the actual grades from the expected results might potentially indicate cheating behavior. (Opgen-Rhein et al., 2018) present an application for detecting plagiarism in programming exams; this app also needs to be trained with previous assignments of a class to recognize authorship of an exam.

Alternatively, (Kassem et al., 2015) propose an approach that requires a formal model of the e-exam system specifications, using Quantified Event Automata, and system logs obtained during the execution of an e-exam. The so called *runtime verification* consists in analyzing actual logs of exam executions to detect discrepancies w.r.t. the specifications, evidencing the occurrence of cheating scenarios.

Note that a robust detection approach would

necessarily require the establishment of both, policies and a clear process to prosecute the identified cheaters. Moreover, even if these approaches provide conclusive evidence that cheating took place, the final verdict still remains a human decision.

4.3 Discussion and Open Questions

From the literature review, we observe that research in both directions for securing e-exams has advanced independently; in particular, due to the unexpected rise of COVID-19, research on detective techniques has considerably increased and shown advances in the past two years. Yet, preventive and detective approaches seem to be complementary: an ideal e-exam system should be secure against cheating in each step of the process prior and posterior to the test itself, and also enable the detection of unauthorized behavior from the examinees to provide the right answers at the moment of the exam.

To the best of our knowledge, the only attempt to integrate both worlds is the work of (Kassem et al., 2017). The authors combine verification of protocol designs with runtime analysis, to find properties violated during the execution of an exam (e.g. due to implementation errors or misbehavior) even when the protocol specifications comply with such properties.

We are interested in advancing research in this direction. More specifically, we aim at setting formal grounds for the development of preventive solutions that ensure relevant security properties w.r.t cheating during the examination phase.

5 TOWARDS FORMALIZING CHEATING AT EXAMINATION

To develop strategies for preventing and mitigating cheating during the examination phase, first we need to clearly define what is considered as cheating. Here, we take a first step and propose possible unambiguous characterizations of cheating.

We focus on the scenario encompassing the methods in Section 3.2, i.e., examinees performing unauthorized actions during the examination phase in order to give the correct answers. From now on, the term *cheating* will be restricted to this particular scenario.

Regardless of the approach, the following elements need to be identified to provide a formal definition of cheating:

1. Factors characterizing the occurrence of cheating.

2. Adversarial models, i.e., assumptions about the examinee’s capabilities.

Potential characteristic factors could be the time spent per question, or the relation between examinees’ answers. Comparing the time spent per question by different examinees could give insights into whether the answers were shared; for instance, a recurrent submission of y ’s answers right after x ’s could mean that x was sharing the solutions. A significant overlap in the wrong answers of two examinees could be another indicator of cheating behavior, along with continuous change in the answers of an examinee.

An adversarial model sets assumptions about the examinee’s capabilities during the examination, for instance, their ability to communicate with the outside, the possibility to use cameras or other devices, or the possibility to access sources of information. These assumptions can also be derived from the restrictions and policies enforced at the e-exam, e.g., if the exam is open-book, or if the exam is proctored, whether it is on-line or in place, etc. (see Section 2).

Once we have a proper characterization of cheating, we should consider the definition of relevant security properties, potentially in terms of the factors previously identified. In general, we are interested in verifying properties of the form “in this setting, successful cheating is never true”, where the setting is given by the model of an e-exam execution. For instance, a model in which the exam questions are represented independently could allow us to express security properties in terms of observable factors of independent questions over time.

Following the previous considerations, we sketch some formalization approaches. Although these are only initial ideas, they expose potential directions for further development of techniques for the prevention of cheating.

5.1 Cheating as Self-outperforming

The main purpose of an exam is assessing one’s skills and capabilities, and examinees prepare themselves for such an assessment. The most common form of assessment is to answer a list Q of questions picked from a possible set of questions \mathcal{Q} . We assume here a “closed- or multiple-choice” exam where questions are accompanied by a small list of possible answers.

Assuming that Q is kept secret, a difficulty for defining cheating is that all examinees (honest or not) have the same goal: to answer Q correctly. By simply looking at the outcome, that is, at the pairs of questions and answers, without any other investigation such as comparing handwriting, it seems unfeasible to distinguish a fraudulent exercise from an honest

one. The distinction seems to be linked to the examinee answering the questions: an honest one has that ability before the exam whereas a fraudster acquires it during the exam, for instance by copying from unauthorized sources or receiving help. But we do not consider as fraudsters those examinees that are unprepared and that answer questions by guessing. Guessing is a strategy, although not necessarily the best one.

We assume an exam to be organized in phases as in (Dreier et al., 2014) (see also Section 2), and to satisfy *question secrecy* (Giustolisi et al., 2013): questions are not revealed before Examination.

Then, an abstract characterization of cheating can try to compare the answers that an examinee would be able to produce in an ideal environment with those given in the real exam environment. We will not define formal semantics for our characterization, although we hypothesize that it should be feasible, e.g., by using a process algebra like spi-calculus (Abadi and Gordon, 1999)¹.

Let \mathcal{A} be the set of all answers and $\text{corr} : \mathcal{Q} \rightarrow \mathcal{A}$ a function associating a question with its correct answer.² For an examinee a , the function $\text{know}_a : \mathcal{Q} \rightarrow \mathcal{A}$ denotes the answers that a associates to the questions in \mathcal{Q} , as a result of her study or taken from material allowed at the exam, for instance because of an open-book policy.

If a would act in complete isolation, $\text{know}_a(Q)$ are her honest answers. But if at the exam, a does not act in isolation, the set of answers she delivers at the end of the examination phase, $\text{test}_a(Q)$, could be different, and can reveal in comparison whether she has cheated.

Definition 1. *An agent a has cheated if*

$$(\text{know}_a(Q) \cap \text{corr}(Q)) \subset (\text{test}_a(Q) \cap \text{corr}(Q))$$

If we interpret know_a as a ’s honest knowledge, Definition 1 captures the following non exclusive situations: a gains a better knowledge than what her preparation justifies; a achieves an answer sheet that is better than the one she would have been able to produce by herself. A second definition is possible.

Definition 2. *An agent a has cheated if*

$$|\text{know}_a(Q) \cap \text{corr}(Q)| < |\text{test}_a(Q) \cap \text{corr}(Q)|$$

Definition 2, implied by the previous one, is more general. Here, the examinee a improves her number of correct answers in comparison to the number

¹Idea: a ’s answering Q in isolation should produce the same outcome as when a answers Q together with other exam takers acting as colluders suggesting answers.

²More generally, $\text{corr} \subseteq \mathcal{Q} \times \mathcal{A}$ is a database of questions with corresponding answers from where we can instantiate a particular exam Q . To simplify notation, here we assume that in Q each question has only one correct answer.

of correct answers she would have compiled in isolation. Note that the questions that a answers correctly can be different from those that she would have answered correctly in isolation, i.e., $\text{test}_a(Q) \cap \text{know}_a(Q) \cap \text{corr}(Q) = \emptyset$ is possible. What counts is that her grading improves compared to the honest performance.

None of these definitions considers unsuccessful attempts, where a fails to perform better than she would have had by behaving honestly: clumsy attempts at cheating are out of scope here.

Because of know_a , our definition is not operational. Observing know_a , which would require testing a student in isolation and before the real exam, is impractical. Nevertheless, our characterization is consistent with any formalisation that introduces an agent's knowledge, which is quite common in epistemic logic e.g., as in the logic of knowledge and belief (Moser, 1989) used in security. Our definitions offer elements of reflection. For instance, preventing a from cheating suggests hindering any effective communication between her and her peers, or from and to the exterior. Further research on how to design protocols that satisfy security properties according to these definitions remains as future work.

5.2 Cheating as an Expression of Help

Even though cheating is closely tied with human interactions, this aspect is rarely considered for the formal study of cheating scenarios. We believe that an idea worth exploring concerns the study of e-exams as socio-technical systems, in which entities capable of autonomous choices (humans), interact with artifacts designed to achieve a specific function (tools).

In (Bottazzi and Troquard, 2015), the authors propose a formalism based on a logic of *bringing-it-about* (BIAT) (Elgesem, 1997), to express properties of helping behavior in terms of cooperating autonomous agents. BIAT logics are modal logics of agency (intervention) rooted in the idea that an action is better explained by what it achieves. Thus, they are adequate for reasoning over the consequences of an action. In short, they are useful for determining whether an agent (entity) is responsible for the actions that caused an observable situation, while abstracting away the means of action.

5.2.1 Successful Cheating

Informally, (Bottazzi and Troquard, 2015) define *successful help* as “agent y tries to achieve a situation S , and agent x makes sure that, if y is trying to achieve a situation S , then S is the case”. We believe that cheat-

ing can be expressed as a collective action instantiating this definition of help.

Definition 3 (Successful Cheating). *An agent x makes sure that, if an agent y is trying to answer a set of questions Q correctly, then y gives the correct answers to Q ; and indeed it is the case that y is trying to answer Q correctly.*

To give a formalization of Definition 3, we introduce the relevant fragment of BIAT logic:

$$\phi ::= p \mid \neg\phi \mid \phi \wedge \psi \mid E_x\phi \mid A_x\phi$$

where p is an atomic proposition, and x is an element of a finite set of agents. E_x represents “agent x brings ϕ about”, A_x expresses “agent x tries to bring ϕ about”, and p describes some state of the world. Then, Definition 3 can be formalized as

$$E_x(A_y q \implies q) \wedge A_y q$$

where q represents “ x answers Q correctly”.

5.2.2 Attempts at Cheating

There are many variable aspects in the previous characterization of cheating; for instance, whether the help of x is intended or not, whether the role of x in the achievement of q is active or passive, etc.

A couple of interesting variants of Definition 3 are the following, where $M_{xy}, M'_{xy} \in \{A_x, A_y, E_x, E_y\}$:

Fake Cheating occurs when y is able to give the correct answers on their own: $M_{xy}(E_y q \implies q) \wedge M'_{xy} q$.

Tentative Cheating occurs when x tries (instead of makes sure) to help y , in which case, the achievement of ϕ is uncertain: $A_x(M_{xy} q \implies q) \wedge M'_{xy} q$.

We could also think about unintended cheating scenarios, e.g. where x is not aware of or does not agree on y copying the answers.

5.2.3 Models and Decision Algorithms

The BIAT logic proposes a suitable formalism for expressing cheating properties in terms of cooperating autonomous agents, however, to practically reason about them, we still need to define:

1. A framework to model the examination phase of e-exam systems.
2. Algorithms for verification of satisfiability of the properties in such models.

(Troquard, 2014) and references therein give insights into the subject. They propose a world-based semantics where a model of agency and ability consists of worlds, agents, effectivity functions to model situations achievable by coalitions of agents, and a

function indicating which atomic propositions hold in each world.

Troquard also presents an algorithm to decide satisfiability of a BIAT formula in terms of the satisfiability of its sub-formulas. The time complexity is $O(2^n)$, with n being the size of the formula. Remark though, that this algorithm decides the existence of a model that satisfies the formula, while we are interested in knowing whether a formula is satisfied in a specific model—a certain e-exam setting.

Presumably, model checking techniques can be used for BIAT by mechanizing the truth value conditions of the language in the semantics. The work of (Kacprzak et al., 2004) could be a reference in this direction.

5.3 Cheating as Information Flow

With information flow, here we mean the flow of answers in a spatial and temporal structure. For this purpose we can resort to spatial-temporal logic.

Spatial-temporal logic extends temporal logic with modalities for expressing topological or metrical relationship, such as adjacency, connectivity, and distance. For instance, VoxLogica (Belmonte et al., 2019) gained attention as an instrument to analyze images, but the logic at the core of the tool can model spatial properties of messages over a graph of connected nodes which, we believe, makes it useful to define spatial-temporal information flow properties in the context of exam cheating.

In several settings, such as in a classroom or in remote exams over a secured browser, it is possible to trace both the position of examinees and the history of their answering, i.e., which questions they answered and in which timestamped order. With such pieces of information, cheating could be expressed as a spatial-temporal property over the flow of answers. For instance, in an exam where questions are presented in a distinct randomized order to each examinee, the presence of a source of information with a flow that regularly expands towards the outside, like in a spanning tree, may suggest a person passing answers to the others, and then forwarding the answers further. Answers that appear almost instantaneously and ubiquitously could suggest a colluding teacher dictating answers to the classroom, as it happened in a scandal that involved the English Testing Service (ETS) a few years ago³.

³BBC, “Student VISA system fraud exposed in BBC investigation”, 2014, URL: <https://www.bbc.com/news/uk-26024375>, visited the 29/11/2021

6 FURTHER DIRECTIONS

We have presented insights into three formal characterizations of cheating during the examination phase, addressing individual and group cheating. The formalization approaches have potential to be developed further for the formal study of cheating scenarios, with the final goal of developing e-exam systems resilient to cheating during the examination phase.

We have also identified multiple open questions and ideas for follow up research, some of which we discuss next.

Remarkably, neither for prevention nor for detection of cheating, there exists an approach that addresses the representation of the human interaction in a formal language; consequently, there is no technique that allows to carry out a formal analysis considering the interaction of the human element. We believe this to be an important research direction as it would bring insights from a, usually less studied, socio-technical security perspective.

We also believe that the works of (Kassem et al., 2015) and (Kassem et al., 2017) mentioned in Section 4 present a promising direction for detecting collusion among students. The authors already suggest a way to address this by looking at similar answer patterns. Yet, given that the technique is based on events observed from an exam execution, the properties that can be verified are limited by the logs recorded by the e-exam system in place. Hence, a necessary first step would be to determine and log relevant information.

We consider the parallel study of group-cheating and individual-cheating. In the former, a group of examinees engage in collective cheating behavior willingly sharing answers; in the latter, one person gets the knowledge from any source (possibly other examinees) without any action from the sources. We believe that the differences in the dynamics of the behavior and in the flow of information could make group-cheating easier to characterize and analyze.

Finally, there are various formalisms and concepts in game theory that focus on cheating and that could be applied to the analysis and formalization of secure e-exams. We encourage research in this direction.

ACKNOWLEDGEMENTS

This research is supported by the Luxembourg National Research Fund, within the project “Secure and Verifiable Test and Assessment Systems (Severitas)”.

REFERENCES

- Abadi, M. and Gordon, A. D. (1999). A calculus for cryptographic protocols: The spi calculus. *Information and computation*, 148(1):1–70.
- Awad Ahmed, F. R., Ahmed, T. E., Saeed, R. A., Al-humyani, H., Abdel-Khalek, S., and Abu-Zinadah, H. (2021). Analysis and challenges of robust e-exams performance under covid-19. *Results in Physics*, 23.
- Backman, J. (2019). Students’ experiences of cheating in the online exam environment. Bachelor thesis, Laurea University of Applied Sciences.
- Bella, G., Giustolisi, R., Lenzini, G., and Ryan, P. Y. (2015). A secure exam protocol without trusted parties. In *IFIP International Information Security and Privacy Conference*, pages 495–509.
- Belmonte, G., Ciancia, V., Latella, D., and Massink, M. (2019). Voxlogica: A spatial model checker for declarative image analysis. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, pages 281–298.
- Bjorklund, M. and Wenestam, C.-G. (1999). Academic cheating: frequency, methods, and causes. *European Conference on Educational Research, Lahti, Finland*.
- Bottazzi, E. and Troquard, N. (2015). On help and interpersonal control. In *The Cognitive Foundations of Group Attitudes and Social Interaction*, pages 1–23. Springer.
- Castella-Roca, J., Herrera-Joancomarti, J., and Dorca-Josa, A. (2006). A secure e-exam management system. In *First International Conference on Availability, Reliability and Security (ARES’06)*, pages 8–pp. IEEE.
- Dawson, P. (2016). Five ways to hack and cheat with bring-your-own-device electronic examinations. *British Journal of Educational Technology*, 47(4):592–600.
- DiSario, R., Olinsky, A., Quinn, J., and Schumacher, P. (2009). Applying monte carlo simulation to determine the likelihood of cheating on a multiple-choice professional exam. *Case Studies In Business, Industry And Government Statistics*, 3(1):30–36.
- Dreier, J., Giustolisi, R., Kassem, A., Lafourcade, P., and Lenzini, G. (2015). A framework for analyzing verifiability in traditional and electronic exams. In *International Conference on Information Security Practice and Experience*, pages 514–529. Springer.
- Dreier, J., Giustolisi, R., Kassem, A., Lafourcade, P., Lenzini, G., and Ryan, P. Y. (2014). Formal analysis of electronic exams. In *2014 11th International Conference on Security and Cryptography (SECRYPT)*, pages 1–12. IEEE.
- Dsouza, K. and Siegfeldt, D. (2017). A conceptual framework for detecting cheating in online and take-home exams. *Decision Sciences Journal of Innovative Education*, 15.
- Elgesem, D. (1997). The modal logic of agency. *Nordic Journal of Philosophical Logic*.
- Fan, Z., Xu, J., Liu, W., and Cheng, W. (2016). Gesture based misbehavior detection in online examination. In *2016 11th International Conference on Computer Science & Education (ICCSE)*, pages 234–238. IEEE.
- Furnell, S. and Karweni, T. (2001). Security issues in online distance learning. *Vine*.
- Giustolisi, R., Lenzini, G., and Bella, G. (2013). What security for electronic exams? In *2013 International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pages 1–5. IEEE.
- Guénard, F. (2012). *La Fabrique des Tricheurs*. J.-C. Gawsewitch.
- Huszti, A. and Petho, A. (2010). A secure electronic exam system. *Publicationes Mathematicae Debrecen*, 77(3-4):299–312.
- Kacprzak, M., Lomuscio, A., Łasica, T., Penczek, W., and Szreter, M. (2004). Verifying multi-agent systems via unbounded model checking. In *International Workshop on Formal Approaches to Agent-Based Systems*, pages 189–212.
- Kamalov, F., Sulieman, H., and Santandreu Calonge, D. (2021). Machine learning based approach to exam cheating detection. *Plos one*, 16(8).
- Kassem, A., Falcone, Y., and Lafourcade, P. (2015). Monitoring electronic exams. In *Runtime Verification*, pages 118–135. Springer.
- Kassem, A., Falcone, Y., and Lafourcade, P. (2017). Formal analysis and offline monitoring of electronic exams. *Formal Methods in System Design*, 51(1):117–153.
- Li, M., Luo, L., Sikdar, S., Nizam, N. I., Gao, S., Shan, H., Kruger, M., Kruger, U., Mohamed, H., Xia, L., and Wang, G. (2021). Optimized collusion prevention for online exams during social distancing. *npj Science of Learning*, 6.
- Moser, L. (1989). A logic of knowledge and belief for reasoning about computer security. In *Proc. of the Computer Security Foundations Workshop II*, pages 57–63.
- Moten Jr, J., Fitterer, A., Brazier, E., Leonard, J., and Brown, A. (2013). Examining online college cyber cheating methods and prevention measures. *Electronic Journal of E-learning*, 11(2):139–146.
- Opgen-Rhein, J., Küppers, B., and Schroeder, U. (2018). An application to discover cheating in digital exams. In *Proc. of the 18th Koli Calling International Conference on Computing Education Research*, pages 1–5.
- Schneider, S., ETH Zurich, and Educational Development and Technology (LET) (2010). Safe exam browser. https://safeexambrowser.org/about_overview_en.html.
- Sindre, G. and Vegendla, A. (2015). E-exams versus paper exams: A comparative analysis of cheating-related security threats and countermeasures. *Department of Computer and Information Science (IDI)*, 8.
- Søgaard, T. M. (2016). Mitigation of cheating threats in digital byod exams. Master’s thesis, NTNU.
- Troquard, N. (2014). Reasoning about coalitional agency and ability in the logics of “bringing-it-about”. *Autonomous Agents and Multi-Agent Systems*, 28(3):381–407.