# Observations of Cheating Behaviours in Online Examinations and Tools for Mitigation

Manuel Castro*, Sathiamoorthy Manoharan†, Ulrich Speidel†, Xinfeng Ye†, and Jiayi Zu†
*Universidad Nacional de Educacion a Distancia,
Madrid,
Spain
†School of Computer Science, University of Auckland,
Auckland,
New Zealand

***Abstract*—The Covid-19 pandemic necessitated a rapid transition to online education, forcing most academic institutions to adopt online assessments as a substitute for traditional, in-person examinations. Many of these online assessments were conducted in an unsupervised setting, with an underlying model that largely relied on the trust that students would maintain academic integrity and adhere to the principles of honest scholarship. Unfortunately, this trust-based approach showed its vulnerabilities, as we observed a significant uptick in incidents of cheating and academic dishonesty across many educational institutions including our own. In an attempt to address these issues, this paper provides an in-depth analysis of the specific cheating behaviours we have identified. We detail how the lack of supervision in online settings has led to creative and highly collaborative cheating schemes that we call local and remote "exam parties," in addition to the use of online platforms like Chegg.com to contract-cheat. The rise in cheating has been so dramatic that it has led to noticeable grade inflation, skewing academic performance metrics and potentially diminishing the value of educational qualifications. To combat this worrisome trend, we introduce an analysis tool specifically designed to detect signs of potential dishonesty in online assessments. The tool consumes student activity logs from popular Learning Management Systems such as Canvas, and digital assessment platforms such as CodeRunner and Inspera, and analyses these logs to flag suspicious behaviours. Combined with rapid-fire answer submissions and other suspicious timing patterns, the reports generated via the tool help us identify collusion and potential contract-cheating. In addition to the tool, the paper discusses preventive measures that institutions can take to minimize the risk of cheating. These include designing assessments to minimize the ability to cheat, enforcing remote proctoring services, and employing individualized assessments. By combining comprehensive analysis, technological solutions, and preventive recommendations, this paper aims to provide educators and institutions with the tools and knowledge they need to uphold academic integrity in this new era of online education.**

***Keywords*—*online assessments, academic honesty, spatial forensic analysis.***

## I. Introduction

During the Covid-19 pandemic, virtually all academic institutions worldwide were forced to swiftly transition from traditional classroom teaching and examinations to online modes of instruction and assessment. The transition presented numerous challenges, the most daunting of which was the maintenance of academic honesty, as evidenced by multiple studies [1], [2].

Examinations, traditionally conceived and conducted as invigilated, closed-book tests, found little parallel in the new virtual environment, posing significant challenges. The urgent nature of the pandemic, coupled with the limited preparation time, necessitated this abrupt migration of traditional examinations to an online format.

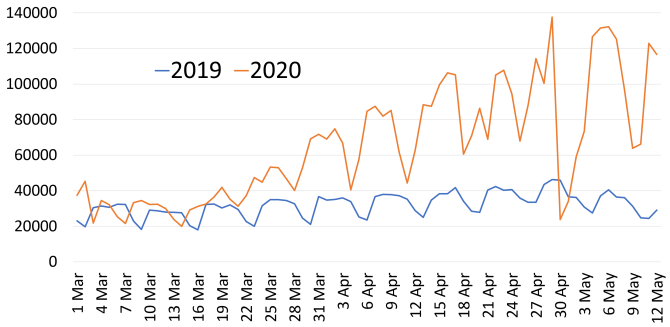


Fig. 1. Questions per day on Chegg. Comparison between years 2019 and 2020 shows substantial increase in the number of questions during the global pandemic lockdowns [3].

Constrained by the lack of resources and the impracticality of virtual proctoring for all online examinations, a substantial number of these tests went uninvigilated. This vacuum led to an unexpected surge in academic dishonesty, with students seeking solutions to questions online or resorting to contract-cheating [4] platforms like Chegg.com. As shown in Fig. 1, the number of questions posted to Chegg.com exponentially increased during the height of the pandemic [3].

Moreover, we identified numerous instances of student collusion and unauthorized collaboration. The objective of

this paper is twofold: to thoroughly examine the mechanisms of such collusion, and to discuss preventive measures that could curtail enabling factors for such collusion.

Almost all academic institutions rely on education-oriented approaches and honor codes to deter academic dishonesty. While pedagogical measures and embedding the value of academic integrity are the best non-punitive deterrents against cheating, the ease of accessing methods to cheat the system may still tempt a few students. If robust detection mechanisms are in place, some students might be deterred by the risk of being caught. Consequently, it becomes essential to safeguard assessments against potential collusion threats and establish mechanisms that can detect instances of collusion when they occur. Therefore, this paper will further delve into some of the preventive measures that could be employed to mitigate the observed cheating mechanisms.

## II. Motivation

Alongside the noticeable rise in detected instances of contract cheating, predominantly involving Chegg.com, we also observed a significant inflation in our course grades. Our evaluation methods are based on criterion-referenced assessments [5], meaning the students' grades directly reflect their demonstrated level of achievement. Consequently, if these assessments indicate a high level of achievement—be it genuine or acquired through cheating—students receive correspondingly high grades. This correlation implies that increased levels of cheating can invariably lead to substantial grade inflation.

For instance, the grade distributions displayed in Fig. 2 and Fig. 3 illustrate this phenomenon of grade inflation for two of our courses. When in-person examinations were conducted in 2019, roughly 45% of the students secured an A or B grade. In stark contrast, when examinations transitioned online in 2020, nearly 90% of the students achieved an A or B grade. Similarly, where over 20% of the students failed the in-person examination in 2019, fewer than 5% of students failed the online examination in 2020.

It is important to note, however, that not all of the grade inflation can be attributed solely to collusion or cheating. The fact that examinations were now open-book and the usage of online resources was allowed, meant that answers could be easily looked up if an examination wasn't carefully designed to mitigate such an eventuality. Furthermore, several universities, ours included, allocated a more generous time-frame for the examinations. This decision was made in consideration of the practical difficulties faced by students such as poor home internet connections and geographical displacement across different time zones (e.g., many international students went home during the pandemic lockdowns). This meant students potentially had more time to study and comprehend the material just in time to solve the questions, if required.

Given these variables, our primary motivation is to determine the extent to which collusion and cheating

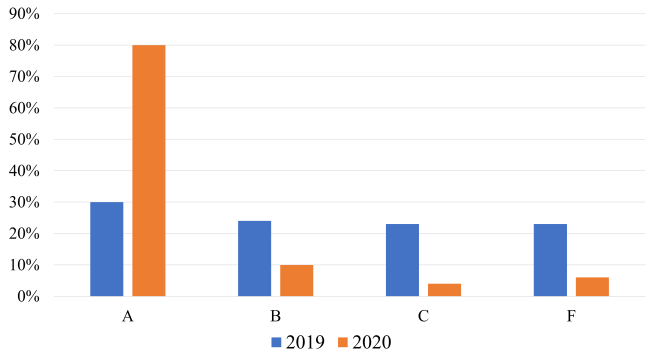


Fig. 2. Grade distributions in in-person supervised (2019) vs. online unsupervised (2020) exams for Course A. The online unsupervised exam sees 80% of the class obtaining A grades while the in-person supervised exam in the previous year only had 30% of the students obtaining A grades.

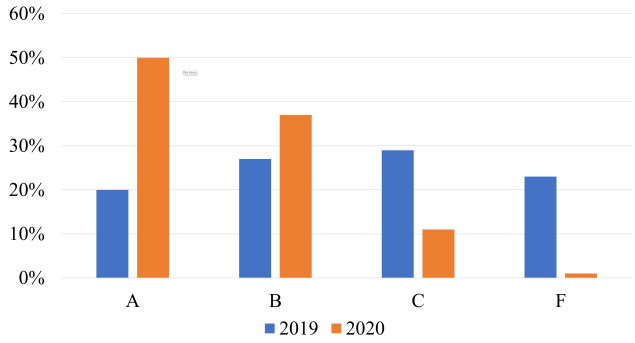


Fig. 3. Grade distributions in in-person supervised (2019) vs. online unsupervised (2020) exams for Course B. The online unsupervised exam sees over 85% of the class obtaining A or B grades while the in-person supervised exam in the previous year only had 45% of the students obtaining A or B grades. Nearly 25% of the students failed the in-person supervised exam, while only 1% of the students failed the online exam.

may have contributed to the observed grade inflation. To achieve this, we conducted a detailed analysis of assessment logs to spot anomalies [6]. Further, we developed a tool to automate this analysis, accelerating the detection and scrutiny of potential collusion or cheating instances.

## III. Local Exam Parties

One of the observed collusion behaviours in online examinations is a *local exam party*, where some students gather in one place to collaboratively solve the exam questions. Most online assessment platforms record the IP addresses of the users, so students' IP addresses can be obtained from these platforms. A local exam party is characterized by many students sharing the same IP address.

While sharing an IP address with another student is a potential indicator of a local exam party, it doesn't necessarily mean that collusion has occurred. For instance, students sharing accommodations are likely to have the same IP address during their examinations. In fact, there

are several contexts where a shared IP address could be purely coincidental. In our case, the most common situations of this kind were the shared exit point of a VPN (Virtual Private Network) service that the university provided for its students in China, and students being assigned the same public IP address by the university's Carrier-Grade Network Address Translators (CGNATs) when accessing the assessment platforms from a student lab or campus WiFi.

## IV. Remote Exam Parties

Another observed collusion behaviour is a *remote exam party*, where a student is observed using multiple IP addresses, sometimes spread across several geographical regions. Each student in a remote exam party would solve a subset of questions for all the students in the party. Multiple IP addresses may also be seen when a student hires one or more substitutes to engage in contract cheating.

However, there are legitimate uses for multiple IP addresses.

Many individuals now use multiple devices. If, for example, a student uses a phone connected to a mobile service provider and a computer connected to a home network during an examination, two IP addresses would be observed. This is typically not a concern, and we know from students that they have used up to six separate devices.

Some countries require students to use a VPN to access services abroad – we have already mentioned this for China. Exit nodes of such VPNs may change during the examination timeframe, or VPNs may become unavailable when detected. This could result in a student appearing to have multiple geographically distributed IP addresses. This too is not necessarily a concern unless other factors are evident, such as a student being observed accessing from several local IP addresses (e.g., an on-campus one and a fixed-line address from an external ISP) or accessing from both a local and an overseas IP address. Therefore, it can be challenging to distinguish legitimate uses of multiple IP addresses from the illegitimate use in remote exam parties.

Potential collusion attempts arising from local and remote exam parties are not solely spatial, i.e., based on location. Temporal collusion patterns are also commonly observed and can supplement spatial patterns in the forensic analysis. Cleophas and colleagues provide an analysis of temporal patterns [7], proposing two particular patterns: (1) a synchronous pattern where two students attempt answers simultaneously, and (2) a leader-follower pattern where one student (the follower) copies solutions from another student (the leader) as the leader works out the solution. Identifying these patterns requires analysing the answering behaviour of every pair of students in the class, e.g., via a similarity analysis tool such as MOSS[1], TurnItIn[2], or MESS [8] followed by additional analysis of the respective submissions' genesis to identify leaders and followers.

A naïve analysis might only look at single solution submissions over time.

A behaviour we often observe in submissions is that a student will submit a perfect solution, then interactively refactor or reformulate it. For programming questions, this refactoring consists mostly of mundane but unnecessary modifications like changing variable names, swapping 'for loops' with 'while loops' or vice versa, etc. This generally indicates that a solution was copied from someone else, and that the student attempted to avoid detection through obfuscation. For instance, CodeRunner [9], a Moodle-based online programming and assessment environment, logs every submission, making it possible to document the transformation from the generic copied solution to the obfuscated version.

Another behaviour we observe is students arriving at an answer too quickly, indicating that the answer was prepared outside of the assessment platform and pasted in. The assessment logs can help identify this as well, so that an instructor can judge if there is an anomaly.

## V. A Tool for Spatial Forensic Analysis

Most educational tools, such as learning management systems (LMS) and digital assessment platforms, keep logs of student activities. These logs are useful for forensic analysis when there are suspicions of possible collusion.

Our institution uses Canvas[3] as our learning management system and Inspera[4] as the digital assessment platform. However, we conduct some of the assessments using the quiz facility provided by Canvas. The primary difference between Canvas and Inspera, from a forensic perspective, is that students can have multiple concurrent sessions running on Canvas, whereas they can only have a single session at a time on Inspera.

In addition, our computer science courses utilize CodeRunner [9], [10] for a number of programming assessments.

The first analysis tool we developed is designed for Canvas. Fig. 4 illustrates the overall architecture of this analysis tool. Central to the tool is a proxy that acts as the gateway to access student logs using API calls (and an API key). The proxy also serves as the gateway to access other related resources such as IP registration data [11] and location indicators (e.g., world map, country flags).

The online application uses the data from the proxy to generate student reports and course reports for a time interval specified by the instructor. The start and end times for this interval are typically the start and end times of the examination.

[1]https://theory.stanford.edu/~aiken/moss/

[2]https://www.turnitin.com

[3]https://www.instructure.com/canvas

[4]https://www.inspera.com

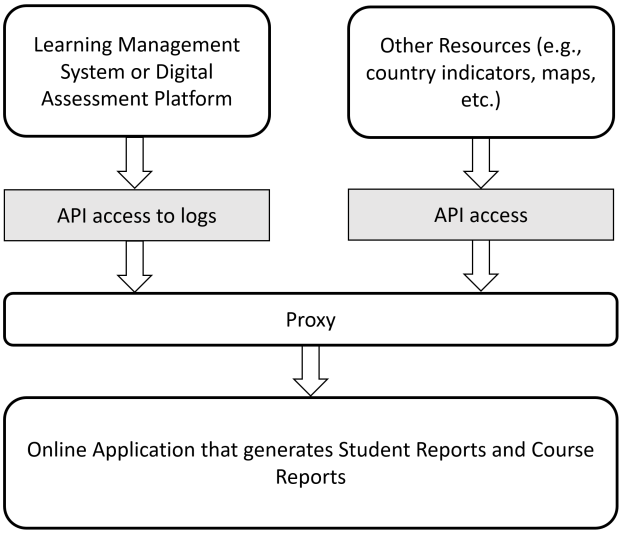


Fig. 4. The architecture of the forensic analysis tool

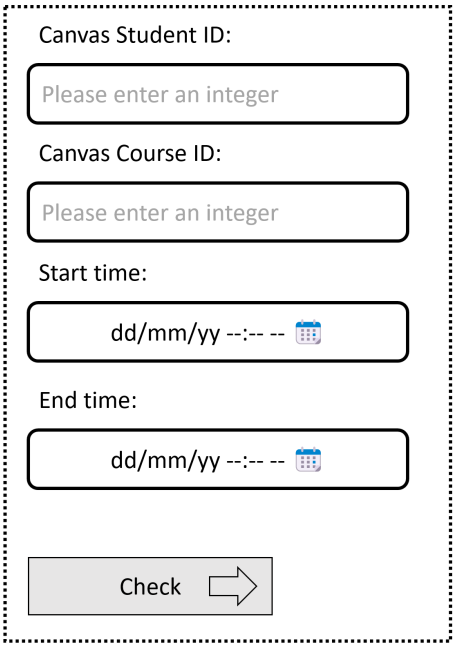


Fig. 5. Application UI for student logs and reports

A student report summarizes the student activity during the specified time interval for a given course. Fig. 5 illustrates the application's minimalistic UI for viewing student reports. This is a spatial report, meaning that it only gathers and reports location information for the student. Student solutions submitted over the course of the examination are not analysed and correlated with the spatial information. The report shows the physical countries associated with the student's IP addresses on a world map. In addition, each access is summarized and annotated with the country flag to highlight the location of the physical country where the IP address originates.

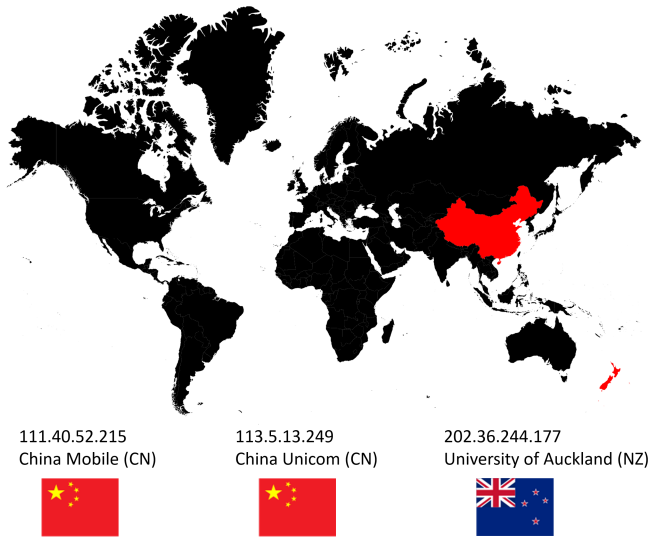


Fig. 6. A sample student report

See Fig. 6 for a sample student report. In this case, the student uses three IP addresses, two from China and one from New Zealand. According to this report, there were three different accesses made to the examination resources during the exam period – two from China and one from New Zealand. The New Zealand IP address used here belongs to the University of Auckland and cannot be a VPN exit node. On this basis, this case should be reported for disciplinary review.

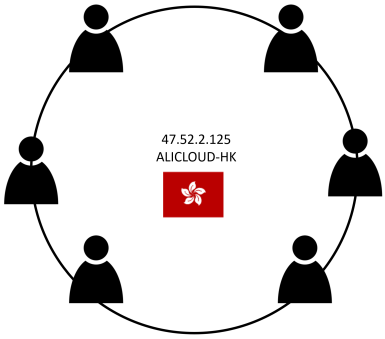


Fig. 7. A sample section of a course report

A course report is a collection of student reports, but it includes additional analysis that reports on the use of shared IP addresses. In other words, it clusters students based on shared IP addresses. The application UI for viewing course logs and reports is similar to the one illustrated in Fig. 6, except that there is no student ID to input. See Fig. 7, which shows one sample cluster of students sharing the same IP address. The shared IP

address used by this cluster is a VPN exit node reserved for use by these students, and is therefore legitimate.

### A. Extending the Analysis to Other Platforms

The principles underpinning this analysis are not exclusive to any single Learning Management System or digital assessment platform. Rather, they can be readily adapted and applied to a variety of such systems, provided that these platforms are capable of maintaining and granting access to logs of student activities.

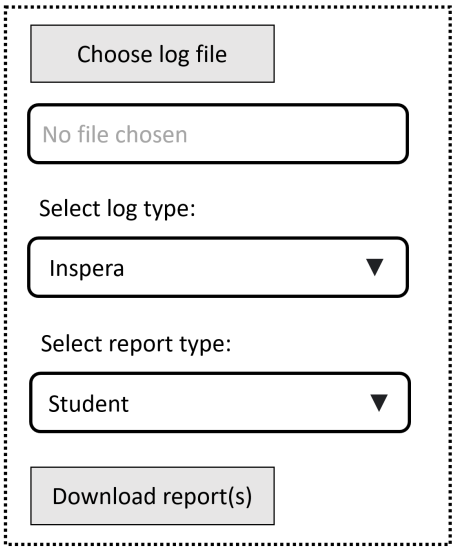


Fig. 8. Application UI for student and course reports for Inspera and CodeRunner

For instance, both Inspera and CodeRunner, which are popular digital assessment tools, keep logs that contain identifiable student information such as student IDs or names. In addition to this, these platforms also log the IP addresses that each student uses to access the assessment. These logs are then utilized in the analysis portion of the forensic tool to produce student reports and course reports, as illustrated in Fig. 6 and Fig. 7, respectively. The student reports are designed to offer a detailed view of each individual student's IP address locations, while the course report provide an aggregate view, compiling data from all the students who participated in a specific assessment.

Fig. 8 illustrates the application's minimalistic UI for generating student and course reports. The UI allows to upload a log file generated by the assessment platform, and downloads either a set of student reports or the course report.

### B. Limitations

At present, the analysis software is designed specifically for Canvas LMS, Inspera, and CodeRunner but the concept could be extended to other learning management systems and digital assessment platforms.

The tool does not currently consider student solutions to check how they correlate with other students' submissions and location data. These checks are manually done based on the student and course reports generated by the tool.

## VI. Preventive Measures

The prevalence of collusion and cheating in online assessments highlights the need for proactive measures. Implementing effective preventive strategies can deter dishonest behaviours and promote academic integrity.

Digital assessment platforms should implement measures to allow a student to use only a single IP address at a time. Such an approach would render the organization of remote exam parties inconvenient, albeit not impossible. For instance, being open-source, CodeRunner has already been modified to operate in a single-session mode. However, implementing such changes can be more challenging when it comes to commercial software.

In terms of assessment design, individualized examinations using an automated platform such as the *R exams package* [12] or Dividni [13] is a scalable approach to mitigate collusion. However, they are not resistant to contract cheating. Oral examinations are quite effective against cheating, but they are not scalable for large classes.

In-person supervised examinations remain the best way to mitigate collusion. When online examinations are unavoidable, the use of remote proctoring should be employed to reduce the likelihood of local and remote exam parties.

It is also important to employ an educational approach to academic integrity. Regular analysis of assessment data to identify potential anomalies, along with the use of plagiarism detection tools, also play an important role.

## VII. Evaluation

Our spatial analysis complements the temporal analysis proposed by Cleophas and colleagues [7] and the content analysis proposed by Johnson and colleagues [14].

The implementation of our spatial analysis tool has already proved to be remarkably effective; it successfully led to the identification of over 60 students who exhibited cheating behaviours during our CS2 examinations. This substantial figure underscores the practical utility and effectiveness of our tool in pinpointing instances of potential academic dishonesty.

As our examination procedures are gradually reverting back to the previously employed invigilated, in-person mode, the tool continues to provide critical support. It has demonstrated its capabilities by identifying instances of shared credentials during in-person assessments, effectively acting as a deterrent against such misconduct. Furthermore, it has been instrumental in refuting false location claims, ensuring the integrity of our assessment procedures.

The reports generated by our tool have broader applications as well. They can serve as an essential resource in

revealing larger, systemic behavioural patterns that may indicate widespread cheating or answer sharing among a substantial student cohort. The course reports, in particular, provide a more overarching view, capturing data at a scale that can influence policy decisions. Therefore, they could be instrumental in shaping institutional guidelines and protocols concerning the maintenance of academic integrity in online as well as in-person assessments.

## VIII. Discussion

Certain learning management systems, most notably Canvas LMS, allow the same student to maintain concurrent logins. This feature presents a loophole where a student, while undergoing a Canvas quiz-based assessment in an invigilated lab, might potentially share their login credentials with an external party. This could enable them to receive unauthorized assistance remotely, circumventing the system's academic honesty measures. The forensic analysis tool we have described in this paper is designed to identify and highlight such instances, thereby helping to uphold the integrity of the assessment process.

Recently, we have also come across cases where students, despite actually residing within the country, falsely claimed to be overseas. The motive for this strategy was to gain access to unsupervised online assessments, rather than participating in the supervised, in-person assessments. These students had a history of previous examination offenses, making them high-risk candidates for the high trust assessment modes employed in online exams. Fortunately, the IP addresses reported by our forensic tool offered us solid evidence to counteract their false claims. The data showed consistent accesses to university resources from New Zealand addresses, including connections made from campus WiFi. These instances of deceit are currently under investigation and undergoing the university's disciplinary process.

## IX. Summary and Conclusion

The Covid-19 pandemic significantly accelerated the shift to online assessments in academic institutions, revealing numerous challenges to maintaining academic integrity. Specifically, the increased prevalence of collusion behaviours, contract cheating, and grade inflation necessitated the development of more robust tools for detecting potential academic dishonesty.

We outlined a tool we developed to help detect potential collusion, based primarily on IP addresses analysis, but acknowledging the complexity and potential fallibility of such a method. While shared IP addresses and multiple geographically distributed IP addresses may be indicative of collusion, they could also be the result of legitimate circumstances such as shared accommodations, VPN usage, or multiple device usage. Further complexity arises in distinguishing between spatial and temporal collusion patterns, such as synchronous or leader-follower behaviours. These necessitate not just IP tracking, but in-depth analysis of the content and progression of students' submissions. Our tool, while centered on spatial detection, still underscores the importance of a more comprehensive approach to collusion detection.

While we are seeing a gradual return to in-person, invigilated assessments, the relevance of the forensic analysis tool persists. It has been useful in identifying cases of shared credentials during in-person assessments and countering false location claims. The tool's continued application could prove beneficial, particularly as academic institutions become more hybrid in their approach to teaching and assessment. However, the tool's current scope is limited to Canvas LMS, Inspera and CodeRunner, and it does not yet analyse student solutions for correlations with other submissions and location data. Future work should therefore focus on extending the tool's functionality to other learning management systems and incorporating an analysis of student solutions.

In light of the challenges presented by online assessments, it is essential to not only develop and improve detection tools but also consider preventative measures. This includes designing open-book assessments effectively and implementing robust measures that encourage a culture of academic honesty among students. For digital assessment platforms, it is important that a student can only use a single IP address at a time, making remote exam parties inconvenient but not impossible. The experience from the pandemic has undoubtedly highlighted the complex task of maintaining academic integrity in an increasingly digital learning environment.

## References


[1] S. Manoharan and X. Ye, "On upholding academic integrity in online examinations," in *2020 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*, 2020, pp. 33–37.

[2] F. Staring, M. Brown, P. Bacsich, and D. Ifenthaler, "Digital higher education: Emerging quality standards, practices and supports," Organisation for Economic Cooperation and Development (OECD, Tech. Rep. 281, 2022.

[3] S. Manoharan, U. Speidel, and X. Ye, "On gaining insights into contract cheating," in *2021 30th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE)*, 2021, pp. 1–4.

[4] T. Bretag, "Contract cheating will erode trust in science," *Nature*, vol. 574, p. 599, October 2019.

[5] T. Burkett, "Norm-referenced testing and criterion-referenced testing," in *The TESOL Encyclopedia of English Language Teaching*. John Wiley and Sons, Ltd, 2018, pp. 1–5.

[6] J. Zu, S. Manoharan, U. Speidel, and X. Ye, "Investigating digital examinations through forensic analysis," in *2023 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2023, p. 4.

[7] C. Cleophas, C. Hönnige, F. Meisel, and P. Meyer, "Who's cheating? Mining patterns of collusion from text and events in online exams," *INFORMS Transactions on Education*, vol. 23, no. 2, pp. 84–94, 2023.

[8] N. Moshiri, "A scalable approach for detecting exam similarity in CS courses," *J. Comput. Sci. Coll.*, vol. 37, no. 10, pp. 8–16, apr 2022.

[9] R. Lobb and J. Harlow, "Coderunner: A tool for assessing computer programming skills," *ACM Inroads*, vol. 7, no. 1, pp. 47–51, Feb. 2016.

[10] D. Croft and M. England, "Computing with CodeRunner at Coventry University: Automated summative assessment of Python and C++ code," in *Proceedings of the 4th Conference on Computing Education Practice*, ser. CEP '20. New York, NY, USA: Association for Computing Machinery, 2020.

[11] C. Ganán, "A primer in registration data access protocol (RDAP) performance," Internet Corporation for Assigned Names and Numbers (ICANN), Tech. Rep. OCTO-024, May 2021.

[12] B. Grün and A. Zeileis, "Automatic generation of exams in R," *Journal of Statistical Software*, vol. 29, no. 10, pp. 1–14, 2009.

[13] S. Manoharan, "Cheat-resistant multiple-choice examinations using personalization," *Computers & Education*, vol. 130, pp. 139–151, 2019.

[14] C. Johnson, R. Davies, and M. Reddy, "Using digital forensics in higher education to detect academic misconduct," *International Journal for Educational Integrity*, vol. 18, no. 1, p. 12, May 2022.