# A Framework for Analyzing Associativity and Anonymity in Conventional and Electronic Summative Examinations

Kissan Gauns Dessai[1(✉)] and Venkatesh Kamat[2]

[1] Department of Computer Science, Government College of Arts, Science and Commerce, Sanquelim, Goa, India
kissangd@gmail.com
[2] Department of Computer Science and Technology, Goa University, Taleigão, Goa, India
vvkamat@unigoa.ac.in

**Abstract.** The prevalence of malpractices in the assessments carried by educational institutions worldwide appears to be very high. Appropriate measures to deter and prevent the malpractices during the examinations are necessary to uphold the academic integrity and to ensure the basic principles of fairness throughout the examination process. Some malpractices such as question paper leakage and collusion/plagiarism can be controlled considerably, if unique question paper is provided to each student/group of students. However, the use of unique question paper for each student/group of students brings up some security and performance challenges non-existent in the examination system with the common question paper. One specific challenge in the examinations with the unique question paper is binding the unique question paper with the answer-script produced by the student and establishing the anonymity of student and examiners from each other. The purpose of this paper is to propose a framework, that establishes and preserves the association between the given question paper and the answer-script and provide required anonymity to students and examiners during an exchange of the examination content. In order to achieve this goal, we first formalize the associativity and anonymity properties and then validate our framework by analyzing the associativity and anonymity properties for the existing conventional/electronic summative examination system.

**Keywords:** Associativity · Anonymity · e-Examination · Question paper · Answer script · Plagiarism · Collusion · Applied $\pi$ calculus · ProVerif

## 1 Introduction

Summative examinations form an integral part of any educational system for grading the students. The summative examination process includes a plethora of activities such as the registration of students, examination fee management,


I. Ray et al. (Eds.): ICISS 2016, LNCS 10063, pp. 303–323, 2016.
DOI: 10.1007/978-3-319-49806-5_16

question bank management, question paper generation, the answer-script management, evaluation, security control, processing and publication of results, re-evaluations and retests. Management of the entire examination system is a circuitous process and is prone to errors and security breaches [4]. Summative examinations also suffers from endemic and ingenious incidents of unfair means and malpractices such as question paper leakage, answer-script plagiarism, unauthorized answer-script alteration and many such malicious acts of the students/other involved stakeholders [12,18]. Malpractices in the examinations appear to be on the rise across the world, but the security regulations and means of implementing them are not universally available and often ineffective as examination cheating have taken incredible, sophisticated and techno-centric dimensions [12].

Question paper leakage and collusion/plagiarism during answer-script production are two commonly occurring dishonest acts in both conventional and electronic examinations [12]. There have been increasing instances of such incidents plaguing the entire educational system. The main cause for the occurrence of such malpractices in large scale is the use of common question paper across all the students answering the particular course paper. Examination authorities normally keep one common question paper for a particular examination course paper due to the difficulties associated in question paper setting, distribution and identification of multiple question papers. Nonetheless, if multiple sets of question papers are used in examination, a suitable mechanism is required to link the question paper and student answer-scripts together to avoid/resolve any future disputes. In conventional examination system, such binding is normally done using common question paper cum answer booklet or identically labeled question paper and answer-script booklet.

In electronic examinations, unique question paper can be generated randomly for each student, just in time (JIT) with the help of an appropriate question bank. Some malpractices related to question paper leakage can be controlled considerably, if unique question paper is provided to each student during examination [20]. If unique question paper is provided to each student/group of students, there is a need to map the student identity to the corresponding question paper. This mapping needs to be strong enough to prevent both the examination authority (sender) and student (receiver) from denying their action in the future. We also require a mechanism for binding the unique question paper received by the student to the corresponding answer-script produced by the student unambiguously. The binding of the unique question paper with the answer-script, needs to be done in such a way that, it satisfies the following security requirements:

1. The answer-script produced by the student is kept hidden from the examination authority.
2. Answer-script produced by the student is made available to the examiner, but the identity of the student and the question paper is hidden from the examiner.

It is essential to ascertain above requirements of anonymity for mitigating any attempts of coercion and biased assessment. Looking at some of the existing

examination specifications and protocols in the literature [7,14,16], we observed that most of the examination models are based on the assumption of the use of common question paper for each course paper. On the other hand, use of unique question paper for each student/group of students brings up some security and performance challenges non-existent in the examination system with the common question paper. Thus, there is a need of a suitable framework and a set of protocols to deal with the examination systems with unique question paper per student. This paper addresses the required goal of establishing the unambiguous association between the question paper and the corresponding answer-script produced by the student and providing anonymity to communicating entities wherever required.

*Contributions:* In this paper, we define a formal framework modelling conventional and electronic examination system and providing an understanding of associativity and anonymity properties for exchange of question papers and answer-scripts. We validate the effectiveness of our framework by modelling and analyzing associativity and anonymity tests using the applied $\pi$ calculus [1] and Proverif [5] tool. The associativity security properties defined in this paper are novel and to the best of our knowledge, no such/similar work has formed the basis of any research in summative examination context.

*Outline:* The next section provides the background details and overview of the related work. Section 3 provides definitions and models for examination protocols. Section 4 describes and formalizes associativity properties, and develops a framework of analysis for them. Section 5 validates the framework. Section 6 draws the conclusions and outlines the future work.

## 2 Background and Related Work

Examination is the process of testing the ability or achievement of the student in any area [15]. Academic examinations is broadly classified into two categories: formative and summative. The formative examinations are designed to improve the student's learning; whilst the summative examinations are the examinations conducted at the end of a course and counts towards the final course mark/grade [19]. Due to the high-stake nature of the summative tests, the summative examination process remains a target for user security challenges [2].

There is a limited study dealing with the subject of academic examinations and the required framework and protocols for conducting summative examinations securely. Some of the existing examination systems, frameworks and security properties are presented in this section. An internet-based examination protocol is proposed by [13] that ensures authentication and conditional anonymity requirements with minimal trust assumption. [7] have made in depth analysis of examination stages of a typical examination system and have identified the authenticity, privacy, correction, secrecy, receipt, copy detection as security requirements that every exam stage must satisfy. They proposed an examination system with the informal definition of security properties based on cryptographic

protocols. [3,16] propose an examination protocol without the need of a trusted third party that guarantees several security properties including anonymity for anonymising the student's test. A formal framework in the applied $\pi$-calculus to define and analyze authentication and privacy requirements for exams through formalization of several individual and universal verifiability properties has been proposed by [10]. The privacy type properties have been studied in depth in other domains such as voting and in auctions. [17] propose formal methods to formalize interactions among engaging parties and properties to be satisfied by the system for payment transactions, transaction security properties, and trust relationships among the parties. [8] proposes a framework for modelling cryptographic voting protocols in the applied $\pi$ calculus, and show how to express the properties of vote-privacy, receipt-freeness and coercion-resistance. [11] suggest a framework to formally verify security properties in e-Auction protocols. In particular, it shows how protocols can be modeled in the applied $\pi$ calculus and how security properties such as different notions of privacy, fairness and authentication can be expressed.

Most of the existing research work in the field of summative examinations, assume the use of common question paper for all the students answering the particular examination course paper. If we intend to address the issue of question paper leakage and collusion/plagiarism acts of students during examination effectively, use of unique question paper per student/group of students appears to be one good solution. The security approaches that exist in the literature become insufficient when we attempt to use multiple question papers for each course paper. We need a mechanism to link the question paper answered by the student to the corresponding answer-script produced by the student unambiguously. It is also desired to keep the identity of the student and corresponding question paper secret from the examiners and the identity of the examiners secret from the students. We also need to keep student answer-scripts hidden from the examination authority for better security.

In this paper, we define a formal framework where we model conventional and electronic examination system. We formalize associativity and anonymity properties relevant for examinations and state the conditions that associativity and anonymity test has to satisfy. We implement the associativity tests in the applied $\pi$ calculus [1] and use Proverif [5] to run an automated analysis along with manual analysis using theorems. As per our best knowledge, no such research work has been done in the field of examinations.

## 3 Summative Examination Model

Summative examination tasks can be broadly classified into 3 main stages, namely: pre-conduct, conduct and post-conduct. The two main activities of the pre-conduct stage are: enrollment of eligible students and question paper production. Initially, examination authority enrolls eligible students for the examination by allocating a unique examination seat number. The question paper production process deals with the appointment of question paper setters, question paper

setting and management and delivery of question papers to the respective examination centers.

The conduct phase of the examination handles activities such as verification of the student identity vis-a-vis registered identity, delivery of question papers and other required material to the students, supervising the students in the examination hall and the collection of the answer-scripts from the students.

The final post-conduct stage of the examination handles tasks such as providing anonymity to the students and examiners, the delivery of the anonymous answer-scripts to the respective examiners for evaluation, evaluation of the answer-scripts, collections of the evaluated answer-scripts from the examiners and final tabulations of marks for grading.

We consider the following description of the examination system to describe the summative examination model: Eligible students enroll for the examination and are assigned unique seat nos. The question paper setters submit a wide variety of questions/question papers pertaining to the particular course paper to the examination authority. The examination system picks up subset of such questions/question paper randomly and presents as examination question paper to the students answering the examination. Students answer the examination in a supervised environment. Proctors/Supervisors monitor and supervise the conduct of the examination. At the end of the examination students submit the answer-scripts corresponding to the question paper to the examination authority. Examination authority allots the collected answer-scripts to the examiners for evaluation after disguising the identity of the student. The examiner evaluates the student answer-scripts and assigns the marks/grades for each answer based on the marking scheme. Examiner identity is not revealed to the students after evaluation of the answer-scripts.

Based on the examination process described above, our examination model is composed of five classes of communicating entities, namely: students, examination authority, paper setters, proctors and examiners. These communicating entities of an examination can be modelled as processes in the applied $\pi$ calculus. These processes communicate via public or private channels. Processes can perform tests and cryptographic operations on the exchanged data using equational theory describing some algebraic properties [6]. The attacker can inject messages of his choice into the public channels and exploit the algebraic properties of cryptographic primitives due to an equational theory. The examination model also handles question papers, answer-scripts and student performance in the examination all bound together with the set of examination protocols providing necessary goals and security requirements.

### 3.1 Examination

We now define examination on the basis of the above description of the summative examination system. The said definition is based on the electronic payment system defined in [17].

**Definition 1** ***(Examination).*** Examination E is defined as unions of the following sets:

$$E = \{SH, N, QP, AS, SP, EP\} \cup Goals \cup Req \cup Sec \tag{1}$$

*where,*

- *SH, SH* $\neq \phi$*, is a set of communicating entities involved in E, namely, students(A), examination authority(B), invigilators(P), paper setters(T) and examiners(X).*
- *N,* $N \neq \phi$*, is the communication channel used by stakeholders to communicate.*
- *QP is the question paper delivered to the students during the examination.*
- *AS represents answer-script produced by the student at the end of the examination.*
- *SP represent student consolidated performance in the examination.*
- *EP is the examination primitives required for exchange of the examination content. In general, EP represents an examination protocol in E.*
- *Goals represent the set of goals of the stakeholders during the execution of the examination primitives EP.*
- *Req represent the set of requirements of the stakeholders during the execution of the examination primitives EP.*
- *Sec represents the security properties desired in the given examination system.*

Definition (1) models a general examination system. As per our definition, examination stakeholders, question paper, answer-script, student performance and the examination action primitives form the main elements of the system. The goals, requirements and the security properties make the system useful and trustworthy.

### 3.2 Examination Primitives

**Definition 2** ***(Examination Primitives).*** Examination primitives, EP, specify the processes executed by the examination stakeholders to achieve the goals of the system. These are the actions required for exchange of question paper/answer-scripts and other examination related content, amongst stakeholders, SH. In general EP is the examination protocol, It can be represented as:

$$EP = \{SH, QP, AS, SP, N, OP\} \tag{2}$$

*where,*

- *SH, SH* $\neq \phi$ *is the set of communicating entities.*
- *QP represents question paper student needs to answer in the examination.*
- *AS represents answer-script produced by the student at the end of the examination.*
- *SP represent student consolidated performance in the examination.*
- *N, is the communication channel used by stakeholders to communicate.*
- *OP is the set of actions required to complete the examination stages.*

*OP, the set of actions required for the delivery of examination content amongst the examination stakeholders such as question paper delivery, answer-script delivery, evaluated answer-script delivery and result tabulation and declaration.*

### 3.3 Requirements of Communicating Entities

We, in this paper focus on the specific requirements of main entities, namely, student, examination authority and examiner as stated below:

1. The question paper received by the student shall not in any way reveal the identity of the student to anybody.
2. The answer-script produced by the student shall not in any way reveal the identity of the student to anybody.
3. The unique question paper provided to the student and the answer-script produced by the student shall be linked together securely.
4. The answer-script produced by the student shall not be available to any person, except the examiner concerned.
5. The identity of the student and answer-script produced by the student shall not be available together to any person (other than the student).
6. The identity and evaluation carried by the examiner shall not be available together to any person (other than the examiner).
7. The unique question paper provided to the student and answer-script produced by the student shall be linked together securely.

Along with the above identified security requirements, other requirements like confidentiality, non-repudiation etc., are equally important and are well satisfied by our examination model.

### 3.4 Examination Security

**Definition 3** ***(Examination Security).*** Examination System, E must satisfy the following set of security properties, Sec:

$$\begin{aligned} Sec = \{&Authentication, Confidentiality, Integrity, Availability, \\ &Non-repudiation, Verifiability, \boldsymbol{Anonymity}, \boldsymbol{Associativity}\} \end{aligned} \tag{3}$$

*In this paper, we focus on two essential security aspects of examination, namely, associativity and anonymity along with verifiability, where in,*

1. *Anonymity is the state of being not identifiable within a set of entities. In examination system, it is required to keep the identity of certain stakeholders secret to ensure fairness.*
2. *Associativity is the ability to unambiguously link the response and reply actions of students and examination authority (question paper and answer-script) and present only the required information to the involved stakeholder without breaking the link (refer Sect. 4 for detail).*
3. *Verifiability is the ability to record the crucial evidence about events/actions carried by examination stakeholders to assist in dispute resolution.*

## 4 Associativity and Anonymity

When unique question paper is used in the examination, we need a mechanism to associate uniquely the question paper received by the student to the answer-script produced by the student. In this paper, we introduce and define *associativity* property to establish such unique and inseparable bonding between the question paper and the answer-script. We also define anonymity properties to prevent any tracing of student identity based on the uniqueness of the question paper. Student anonymity is required before the marking/grading to prevent any attempts of coercion and favoritism.

### 4.1 Associativity and Anonymity Properties

In this section, we define associativity & anonymity properties required during the exchange of unique question paper & answer script between the stakeholders, namely: examination authority, students and examiners.

**Definition 4** ***(Question paper & Answer-script Associativity).*** *An examination system with student process A (QP, AS, id) and examination authority process B offers question paper & answer-script associativity, if it is possible to unambiguously distinguish when a student $A_1$ produce answer-script $AS_{A_2}$ corresponding to the received question paper $QP_{A_1}$ from the case where examination authority/student claim of producing $AS_{A_2}$ corresponding to altogether different question paper $QP_{A_2}$. This is formally specified by:*

$$\upsilon\tilde{n}.(A\{QP_{A_1}/x, AS_{A_2}/y, A_1/z\}|B) \not\approx_l \upsilon\tilde{n}.(A\{QP_{A_2}/x, AS_{A_2}/y, A_1/z\}|B) \quad (4)$$

An examination system with question paper & answer-script associativity is capable of unambiguously distinguishing between received question paper/answer-script pair from any malicious/false claims. This association is required to build a reliable evidence for resolution of any dispute related to question paper/answer-script originality/correctness.

**Definition 5** ***(Answer-script Secrecy).*** *An examination system with student process A (QP, AS, id) and examination authority process B offers an answer-script secrecy, if it is not possible for the examination authority to distinguish the answer-scripts received. This is formally specified by:*

$$\upsilon\tilde{n}.(A\{AS_{A_1}/x, AS_{A_2}/y\}|B) \approx_l \upsilon\tilde{n}.(A\{AS_{A_2}/x, AS_{A_1}/y\}|B) \quad (5)$$

An examination system with answer-script secrecy ensures that answer-scripts remain hidden from the examination authority. This is desired because examination authority has no role to play in the answer-script evaluation.

**Definition 6** ***(Answer-script Anonymity).*** *An examination system with examination authority process B (QP, AS, pseudo_id) and examiner process X, ensures answer-script anonymity, if it is not possible for the examiners to find the author of the answer-scripts from the received answer-scripts, i.e., student $A_1$*

*producing an answer-script $AS_{A_1}$ is indistinguishable from student $A_2$ producing an answer-script $AS_{A_2}$. This is formally specified by:*

$$v\tilde{n}.(B\{\{AS_{A_1}, pid_{A_1}\}, \{AS_{A_2}, pid_{A_2}\}\}|X) \approx_l v\tilde{n}.(B\{\{AS_{A_2}, pid_{A_1}\}, \{AS_{A_1}, pid_{A_2}\}\}|X) \tag{6}$$

An examination system with answer-script anonymity ensures that, the examiner cannot infer the author of the answer-scripts from the given answer-scripts. Answer-script anonymity is required to prevent any attempt of the student and examiner from coercing with each other and trace the answer-script of the student based on the known student identities and the given answer-scripts.

**Definition 7** ***Examiner Anonymity before Answer-script Evaluation.*** *An examination system with student process A(QP, AS, id) and examination authority process B or examination authority process B(QP,AS,pid), examiner process X and student process A, ensures examiner anonymity before answer-script evaluation from the student(A), if the assignment of $AS_{A_1}$ to examiner $X_1$ for evaluation is indistinguishable from the case where examiner $X_2$ evaluates the answer-script $AS_{A_2}$.*

$$\begin{aligned} &v\tilde{n}.(A\{(AS_{A_1}/x_1, X_1/y_1), (AS_{A_2}/x_2, X_2/y_2)\}|B) \approx_l \\ &v\tilde{n}.(A\{(AS_{A_2}/x_1, X_2/y_1), (AS_{A_1}/x_2, X_1/y_2)\}|B) \end{aligned} \tag{7}$$

*or*

$$\begin{aligned} &v\tilde{n}.(B\{(AS_{A_1}/x_1, X_1/y_1), (AS_{A_2}/x_2, X_2/y_2)\}|X|A) \approx_l \\ &v\tilde{n}.(B\{(AS_{A_2}/x_1, X_2/y_1), (AS_{A_1}/x_2, X_1/y_2)\}|X|A) \end{aligned} \tag{8}$$

An examination system with examiner anonymity before answer-script evaluation ensures that, the identity of the examiner evaluating the answer-scripts cannot be inferred by the students before the completion of the evaluation activity.

**Definition 8** ***Student Anonymity.*** *An examination system ensures student anonymity from the examiners(X), if for any examination process P, with student's identity, $A_1, A_2, ..., A_n$, question papers, $QP_1, QP_2, ..., QP_n$ and answer-scripts, $AS_1, AS_2, ..., AS_n$, where student identities are available to the examiner in isolation, then student identity and corresponding question paper/answer-script is indistinguishable to the examiner(X).*

Student anonymity states that, it should not be possible for the examiners to find the link between given question paper/answer-script and the corresponding student.

## 5 Evaluation of Existing Frameworks

In this section, we evaluate the existing summative examination frameworks, namely: conventional and electronic summative examination system to verify whether they satisfy the formal model presented in the Sect. 3 and associativity and anonymity properties defined in Sect. 4.

### 5.1 Conventional Summative Examination

The conventional summative examination system under our consideration features 5 distinct stakeholders, namely: students (A), examination authority (B), paper setters (T), proctors (P) and examiners (X). The entire examination process is divided into three broad stages: pre-conduct, conduct & post-conduct.

**Examination Stages:** (i) Pre-Conduct:
Pre-conduct stage of the examination deals with registration of eligible students, admission card and unique seat no. generation, question paper setting, appointment of paper setters (at least 3 paper setters for each course paper for guarding the secrecy of question paper), paper production (selecting one question paper randomly from the 3 sets of question paper), provision on answer-books for hiding the identity of student from examiners.

(ii) Conduct:
Conduct phase of the examination carries tasks of authentication of students, assertion of the answer-book freshness with the signature of the invigilator, student attendance record maintenance, monitoring the student activities to control in-house malpractices.

(iii) Post-Conduct:
The post-conduct stage of the examination handles student anonymity (by detaching the student identity from answer-book and assigning a unique code to the answer-book), examiner anonymity (evaluation of answer-scripts is carried without revealing examiner identity on the evaluated answer-books), collection of the evaluated answer-scripts from the examiners, marks entry, final tabulation of marks for grading, scrutiny of the unfair means, tabulation of the results and the issuing of the statement of marks to the students.

**Formal Model:** We provide a formal model of the conventional summative examination in ProVerif. The Students (A), Examination authority (B), Paper setters (T) and Examiners (X) form the main entities and are modelled as communicating processes. The examination model is derived from the definition (1). The attacker has complete control of the network, except the private channels: he can eavesdrop, remove, substitute, duplicate and delay messages that the parties are sending one another, and insert messages of his choice on the public channels (like the Dolev-Yao attacker [9]). Threats are captured due to collusions and coercions, assuming the existence of dishonest parties. We first model the cryptographic primitives used in the system and then the examination system itself. The equational theory depicted below models the cryptographic primitives used within the conventional summative examination system.

**Equational Theory:** We adopt the following signature to capture the cryptographic primitives used by the conventional examination system.

$$\Sigma = \{pk, ok, fst, snd, pair, seal, peal, sign, checksign, code, uncode, hash\}$$

pk corresponds to public key generation, ok is a constant. The properties of concatenation and standard encryption and blind signatures are modeled by the following set of equations:

$$peel(seal(m, pk(k)), k) = m \tag{9}$$

$$uncode(code(x, k), k) = x \tag{10}$$

$$checksign(sign(m, pk(k)), sign(m, k)) = ok \tag{11}$$

The term pk(k) denotes the public key corresponding to the private key k in asymmetric encryption. The function *seal/peel* (refer Eq. (9)), is similar to asymmetric encryption/decryption, is used to model that the attacker cannot see the content of the exchanged messages and only authorized entities can open and see the exchanged content. Paper setters use *seal* function to deliver the question papers securely to the examination authority. The examination authority use *peel* function to get the original question papers back. Examination authority use *seal* function to deliver the question papers to the students. Question papers are peeled open by the authorized students (Student representative needs to make sure that the sealed envelope carrying question papers is not tampered). Similar arrangement is required during answer-script exchange between examination authority and the examiners.

The *code* function (refer Eq. (10)), similar to a symmetric encryption scheme is used to disguise the identity of the student from the examiner. The identity is retrieved back during the final tabulation of marks for grading with the reverse function *uncode*. The function *sign* (refer Eq. (11)) is used to obtain the signature of the student, indicating his presence in the examination concerned. The presence of the student in the examination can be verified, in case of dispute with the help of *checksign* function.

**Analysis of Associativity:** We, now analyze conventional examination system using the equational theory as defined above. We analyze associativity tests guided by the properties defined in Sect. 4. We use indistinguishability assertions to prove associativity properties. We consider the following cases to understand whether an association between the given question paper and answer-script is provided by the conventional examination system:

1. Case 1: When common question paper is used across all the students:
2. Case 2: When unique question paper is used for each student/group of the students:
   (a) Scenario 1: All the students are honest and answer the examination without resorting to any malpractice:
   This is an ideal situation and no dispute situation arises needing any security intervention.
   (b) Scenario 2: Some students indulge in malpractice in the form of collusion/plagiarism:
   In this case, a student colludes or plagiarizes the answer-script of neighboring student, i.e., instead of producing answer-script x, it presents answer-script, y (obtained from the neighboring student).

We now show that the conventional examination system does not preserve the association (refer Definition (4)) between the given question paper and answer-script, even when all but one student is dishonest.

**Theorem 1.** *The conventional examination system does not provide* associativity *(refer Definition (4)) between a given pair of question paper and answer-script.*

*Proof:* In order to prove Theorem 1, we need to show that, it is not possible to unambiguously distinguish when a student $A_1$ produce answer-script $AS_{A_2}$ corresponding to the received question paper $QP_{A_1}$ from the case where a student produce answer-script $AS_{A_1}$, when: (i) Common question paper is used, and (ii) Unique question paper is used.

Let us consider the following frames to verify whether a conventional examination system satisfies the associativity:

$$\begin{aligned}
&\varphi_0 = \{pk(B)/v1\}|\{pk(A_i)/v2\}|\{pk(X_i)/v3\}|\{\{seal(QP_i, A_i)|i = 1..n\},\\
&\varphi_1 = \varphi_0|\{AS_{A_2}/y\},\\
&\varphi_2 = \{AS_{A_1}/y\},\\
&\varphi_k = \{\varphi_{k-1}\}|\{seal((AS_{A_i}, A_i), pk(B))\}|\{seal((AS_{A_i}, pid_i), pk(X))\},\\
&\varphi_\delta = \varphi_n|\{peel((AS_{A_i}, A_i), B)\}|\{peel(AS_{A_i}, pid_i), X)\}
\end{aligned} \tag{12}$$

$\varphi_0$ corresponds to the initial knowledge of the communicating entities. It contains the public data exchanged and the public keys.

$\varphi_1$ corresponds to answer-script submitted by the dishonest student $A_1$.

$\varphi_2$ corresponds to the claim of the examination authority/student after the submission of the answer-script.

$\varphi_k$ corresponds to the knowledge of the examination authority/examiners after the submission of the answer-script by the student $A_1$.

$\varphi_\delta$ corresponds to the opening of the received answer-scripts.

Here, $pid_i$ is the pseudo identity of the student. The actual identity of the student is hidden from the examiners.

*Case 1:* Common question paper $QP_1$ is used:
In this case since all students are answering same question paper, dishonest students can exploit this vulnerability and indulge in plagiarism/collusion. In this situation, since neither party maintains any undeniable evidence which can prove the given answer-script is plagiarized or not (Refer Eq. (12)), it is not possible to fully endorse the claim of any of the communicating entities in case of dispute.

We modelled the conventional examination system with common question paper in Proverif and found that, if the given pair of question paper and answer script is swapped, it remains indistinguishable, i.e., it satisfies observational equivalence as indicated in Eq. (13).

$$P[QP_{A_1}/x, AS_{A_1}/y|QP_{A_1}/x, AS_{A_2}/y] \approx P[QP_{A_1}/x, AS_{A_2}/y|QP_{A_1}/x, AS_{A_1}/y] \tag{13}$$

*Case 2:* Unique question paper is used for each student/group of students: In this case in the event when a student plagiarizes the answer-script of the other student, corresponding to the altogether different question paper, the simple mapping of the student question paper and answer-script cannot act as an undeniable evidence in case of dispute. The conventional examination system does not maintain any undeniable evidence to tackle this issue (refer Eq. (12)).

We modelled the conventional examination system with unique question paper in Proverif and found that, if the given pair of question paper and answer script is swapped, it remains indistinguishable, i.e., it satisfies observational equivalence as indicated in Eq. (14).

$$P[QP_{A_1}/x, AS_{A_1}/y|QP_{A_2}/x, AS_{A_2}/y] \approx P[QP_{A_1}/x, AS_{A_2}/y|QP_{A_2}/x, AS_{A_1}/y] \tag{14}$$

Thus, we state that, the conventional examination system does not provide undeniable evidence for maintaining the association between the question paper received by the student and answer-script produced by the student.

**Analysis of Anonymity:** We, now analyze anonymity properties using equational theory, guided by the properties defined in Sect. 4 and Eqs. (12). We assume the use of unique question paper for each student/group of the students.

**Lemma 1.** *The conventional examination system does not provide* answer-script secrecy *from the examination authority (refer Definition (5)).*

*Proof:* In order to prove Lemma 1, we need to show that, it is possible for the examination authority to distinguish the received answer-scripts from each other. Based on the equational theory and local knowledge of the examination authority (B) (Refer (12)), we propose the following inference system.

$$\frac{B \qquad seal((AS_{A_i}, A_i), pk(B))}{(AS_{A_i}, A_i)}$$

The above inference system clearly indicates that, the examination authority is in a position to access the answer-scripts and student identity as received from the student entity. In other words, each answer-script submitted by the student can be accessed by the examination authority, i.e., each received answer-script is observationally different for the examination authority as indicated in Eq. (15).

$$P[\{AS_{A_1}/x, AS_{A_2}/y\}] \not\approx [\{AS_{A_2}/x, AS_{A_1}/y\}] \tag{15}$$

Thus, we state that, the conventional examination system does not provide secrecy of the answer-scripts from the examination authority.

**Lemma 2.** *The conventional examination system provides* answer-script anonymity *from the examiners (Refer Definition (6)).*

*Proof:* In order to prove Lemma 2, we need to show that, it is not possible for the examiners to find the authors of the answer-scripts from its knowledge base. Based on the equational theory and local knowledge of the examiners (X) (Refer (12)), we propose the following inference system.

$$\frac{X \qquad seal((AS_{A_i}, pid_i), pk(X))}{(AS_{A_i}, pid_i)}$$

Examination authority, send the pseudo identity of the student ($pid_i$) to the examiners. The private key required to reveal the student identity back is known to only the examination authority. In other words, though examiners get the answer-scripts for evaluation, student identity is not available to the examiners during evaluation, i.e., two given answer-scripts are observationally equivalent to the examiners in the absence of knowledge of actual student identity as indicated in Eq. (16).

$$P[AS_{A_1}/x, pid_{A_1}/y | AS_{A_2}/x, pid_{A_2}/y] \approx P[QP_{A_1}/x, pid_{A_2}/y | AS_{A_2}/x, pid_{A_1}/y] \tag{16}$$

Thus, we state that, the conventional examination system provides answer-script anonymity from the examiners.

**Lemma 3.** *The conventional examination system provides* examiner anonymity before answer-script evaluation *from the student entity(Refer Definition (7)), provided answer-scripts are evaluated by the multiple examiners.*

*Proof:* In order to prove Lemma 3, we need to show that, it is not possible for the students to find the identity of the examiners before answer-script evaluation.

We assume that answer-scripts of a particular course paper are allotted to the multiple examiners for evaluation. Based on the equational theory and local knowledge of the students ($A_i$) (Refer (12)), we propose the following inference system.

$$\frac{A_i \quad pk(B) \quad pk(X) \qquad (AS_{A_i}, A_i)}{seal((AS_{A_i}, A_i), pk(B))}$$

Students at the end of the examination need to submit the answer-books to the examination authority. Students may possess the knowledge of the examiners involved in the evaluation, but that knowledge is not sufficient to find the actual examiner involved in the evaluation of the particular answer-scripts. In other words, when two or more examiners are involved in the evaluation, examiner identity and the answer-script assigned to the examiner is indistinguishable to the student entity as indicated in the Eq. (17)

$$P[AS_{A_1}/x, X_1/y | AS_{A_2}/x, X_2/y] \approx P[AS_{A_1}/x, X_2/y | AS_{A_2}/x, X_1/y] \tag{17}$$

Thus, we can state that a conventional examination system provides *examiner anonymity before answer-script evaluation* from the student entity.

### 5.2 Electronic Summative Examination

We study the electronic examination protocol Remark!, proposed by [14]. The protocol participants are the candidates (C), examiner (E), invigilator (G) and manager (M). The role of the manager is: registration of eligible candidates and examiners, Assignment of question papers for candidates, collection of answer tests, distribution of answer tests to examiners and gather marks. The examination process is broadly classified into registration, testing, grading and notification stages as described below:

**Examination Stages:** (i) Registration:
Manager registers the eligible set of students and examiners for the examination by issuing the pseudonyms. Pseudonyms are generated by the exponentiation mixnets for providing anonymity for the candidates/examiners. A bulletin board is used to publish the pseudonyms, the questions, the tests, and the marks.

(ii) Testing:
The manager generates the test questions and signs them with its private key, and encrypts each test question with the help of a candidate pseudonym before putting it on a bulletin board. At the end, each candidate submits his answer, which is signed with the candidate's private key and encrypted with the public key of the manager. The manager collects the test answer, checks its signature using the candidate's pseudonym, re-signs it, and finally publishes its encryption with the corresponding candidate's pseudonym as receipt.

(iii) Grading:
The manager encrypts the signed test answer with an eligible examiner pseudonym and publishes the encryption on the bulletin board. The corresponding examiner marks the test answer, and signs it with his private key. The examiner then encrypts it with the public key of manager, and submits its marks to the manager.

(iv) Notification:
The manager receives the encrypted evaluation from the examiner, which are decrypted and re-encrypted with the help of the corresponding candidate pseudonym. Then, the mixnet servers deanonymize the candidate's pseudonyms by revealing their secret exponents. Hence the candidate anonymity is revoked. The examiner's secret exponent is not revealed to ensure his anonymity even after the exam concludes.

**Formal Model:** We analyze electronic summative examination system offered through the Remark! protocol, using the applied $\pi$ calculus following similar techniques as the one used in the analysis of the conventional examination system. The equational theory depicted below models the cryptographic primitives used within the Remark! protocol. The equations for encryption and signatures are standard.

**Equational Theory:** We adopt the following signature to capture the cryptographic primitives used by the Remark! protocol.

$$\Sigma = \{pk, aenc, adec, checkpseudo, sign, checksign, hash\}$$

corresponding to public key generation, asymmetric encryption, asymmetric decryption, sign, checksign, and pseudo signature and hash calculation. The properties of standard encryption and pseudo signatures are modeled by the following set of equations:

$$adec(aenc(m, pk(k)), k) = m \tag{18}$$

$$adec(aenc(m, pseudo\_pub(pk(k), rce), r), pseudo\_priv(k, exp(rce))) = m \tag{19}$$

$$checkpseudo(pseudopub(pk(k), rce), pseudo\_priv(k, exp(rce))) = true \tag{20}$$

$$getmess(sign(m, k)) = m \tag{21}$$

$$checksign(sign(m, k), pk(k)) = m \tag{22}$$

$$checksign(sign(m, pseudo\_priv(k, exp(rce))), pseudo\_pub(pk(k), rce)) = m \tag{23}$$

The term pk(k) denotes the public key corresponding to the secret key k in asymmetric encryption. The function *aenc/adec* (Refer Eq. (18)), is asymmetric encryption/decryption. The manager uses *aenc* function to deliver the question papers securely to the candidates. Candidates use *adec* function to get the original question papers back. Candidates use *aenc* function to deliver the answer-scripts to the manager. Answer-scripts are decrypted by the manager using *adec*. The function *checkpseudo* (refer Eq. (20)) is used to check if a pseudonym corresponds to a given secret key. The function *pseudo_priv* is used to decrypt or sign messages, using the secret key and the new generator $g^r$. The pseudonym, which also serves as the test identifier is generated using the function pseudo_pub, which takes in a public key and a random exponent.

**Analysis of Associativity:** We, now analyze the Remark! protocol using the equational theory depicted above. We analyze associativity tests guided by the properties defined in Sect. 4. We consider the following cases to understand whether an association between the given question paper and answer-script is satisfied by the Remark! examination protocol:

1. Case 1: When common question paper is used across all the students:
2. Case 2: When unique question paper is used for each student/group of the students:
   (a) Scenario 1: All the students are honest and answer the examination without resorting to any malpractice:
   This is an ideal situation and no dispute situation arises needing any security intervention.

(b) Scenario 2: Some students indulge in malpractice in the form of collusion/plagiarism:
In this case, a student colludes or plagiarizes the answer-script of neighboring student, i.e., instead of producing answer-script x, it presents answer-script, y (obtained from the neighboring student).

We now show that the electronic examination system modelled through the Remark! protocol preserves the association (Refer Definition (4)) between the given question paper and answer-script, even when all but one student is dishonest.

**Theorem 2.** *The Remark! protocol provides* associativity *(refer Definition (4)) between a given pair of question paper and answer-script.*

*Proof:* In order to prove Theorem 2, we need to show that, it is possible to unambiguously distinguish when a student $A_1$ produce answer-script $AS_{A_2}$ corresponding to the received question paper $QP_1$ from the case where a student produce answer-script $AS_{A_1}$, when: (i) Common question paper is used, and (ii) Unique question paper is used.

Let us consider the following frames to verify whether the Remark! protocol satisfies the associativity:

$$\begin{aligned}
&\varphi_0 = \{pk(B), pk(A_i), pk(X_i), pseudo_B, pseudo_{A_i}, pseudo_{X_i}, aenc(QP_i, pseudo_{A_i}) | i = 1..n\},\\
&\varphi_1 = \varphi_0 | \{AS_{A_2}/y\},\\
&\varphi_2 = \{AS_{A_1}/y\},\\
&\varphi_k = \{\varphi_{k-1}\} | \{aenc((QP_i, AS_{A_i}, pseudo_{A_i}), pk(B)), sign((QP_i, AS_{A_i}, pseudo_{A_i}), priv_{A_i}),\\
&aenc((QP_i, AS_{A_i}, pseudo_{A_i}, pseudo_{X_i}), pseudo_{X_i}), sign((QP_i, AS_{A_i}, pseudo_{A_i}), B)\},\\
&\varphi_\delta = \varphi_n | \{adec((QP_i, AS_{A_i}, pseudo_{A_i}), B)\}
\end{aligned} \tag{24}$$

Refer Eq. (12) for definition of $\varphi_0$, $\varphi_1$, $\varphi_2$, $\varphi_k$ and $\varphi_\delta$. Also, $pseudo_B$ is the pseudo public key of the examination authority, $pseudo_{A_i}$ is the pseudo public key of the students, $priv_{A_i}$ is the pseudo private key of the students, $pseudo_{X_i}$ is the pseudo public key of the examiners. The actual identity of the student is hidden from the examiners.

*Case 1:* Common question paper $QP_1$ is used:
Dishonest students can exploit this vulnerability and indulge in plagiarism/collusion. Since, neither party maintains any undeniable evidence which can prove the given answer-script is plagiarized or not (Refer Eq. (24)) it is not possible to fully endorse the claim of any of the communicating entities in case of dispute.

*Case 2:* Unique question paper is used for each student/group of students:
The Remark! protocol builds an undeniable evidence associating the question paper to the answer-script in the form of $sign((QP_i, AS_{A_i}, pseudo_{A_i})$ (Refer Eq. (24)). Since, manager and student gets signed acknowledgement of receipt of the question paper and answer tests pair from each other, they are not in a position to deny their actions (Refer Eq. (24)).

We modelled the Remark! protocol in ProVerif and found that, if the given pair of question paper and answer script is swapped, it is distinguishable, i.e., swapped and original pair are not observationally equivalent as indicated in Eq. (25).

$$P[QP_{A_1}/x, AS_{A_1}/y|QP_{A_1}/x, AS_{A_2}/y] \not\approx P[QP_{A_1}/x, AS_{A_2}/y|QP_{A_1}/x, AS_{A_1}/y] \tag{25}$$

Thus, we state that, the examination system with the Remark! protocol provide an undeniable evidence for maintaining the association between the question paper received by the student and answer-script produced by the student.

**Analysis of Anonymity:** We, now analyze anonymity using equational theory, guided by the properties defined in Sect. 4 and Eqs. (24). We assume the use of unique question paper for each student/group of the students.

**Lemma 4.** *The electronic examination system with the Remark! protocol does not provide* answer-script secrecy *from the examination authority (Refer Definition (5)).*

*Proof:* In order to prove Lemma 4, we need to show that, it is possible for the examination authority to distinguish the received answer-scripts from each other. Based on the equational theory and local knowledge of the examination authority (B) (Refer (24)), we propose the following inference system.

$$\frac{B \qquad aenc((QP_i, AS_{A_i}, pseudo_{A_i}), pk(B))}{(QP_i, AS_{A_i}, pseudo_{A_i})}$$

The above inference system clearly indicates that, the examination authority is in a position to access the answer-scripts and student identity as received from the student entity. In other words, each answer-script submitted by the student can be accessed by the examination authority, i.e., each received answer-script is observationally different for the examination authority as indicated in Eq. (26).

$$P[\{AS_{A_1}/x, AS_{A_2}/y\}] \not\approx [\{AS_{A_2}/x, AS_{A_1}/y\}] \tag{26}$$

Thus, we state that, the examination system with the Remark! protocol does not provide secrecy of the answer-scripts from the examination authority.

**Lemma 5.** *The electronic examination system with the Remark! protocol provides* answer-script anonymity *from the examiners(refer Definition (6)).*

*Proof:* In order to prove Lemma 5, we need to show that, it is not possible for the examiners to find the authors of the answer-scripts from its knowledge base.

Based on the equational theory and local knowledge of the examiners (X) (Refer (24)), we propose the following inference system.

$$\frac{X \quad priv_{X_i} \qquad aenc((QP_i, AS_{A_i}, pseudo_{A_i}, pseudo_{X_i}), pseudo_{X_i})}{(QP_i, AS_{A_i}, pseudo_{A_i}, pseudo_{X_i})}$$

Examination authority, send the pseudo identity of the student($pseudo_{A_i}$) to the examiners. The pseudo private key required to reveal the student identity back is known to only the student. In other words, though examiners get the answer-scripts for evaluation, student identity is not available to the examiners during evaluation, i.e., two given answer-scripts are observationally equivalent for the examiners as indicated in Eq. (27).

$$P[AS_{A_1}/x, pseudo_{A_1}/y | AS_{A_2}/x, pseudo_{A_2}/y] \approx P[QP_{A_1}/x, pseudo_{A_2}/y | AS_{A_2}/x, pseudo_{A_1}/y] \tag{27}$$

Thus, we state that, the examination system with the Remark! protocol provides answer-script anonymity from the examiners.

**Lemma 6.** *The electronic examination system with the Remark! protocol provides* examiner anonymity before answer-script evaluation *from the student entity (Refer Definition (7)), provided answer-scripts are evaluated by the multiple examiners.*

*Proof:* In order to prove Lemma 6, we need to show that, it is not possible for the students to find the identity of the examiners before answer-script evaluation.

We assume that answer-scripts of a particular course paper are allotted to the multiple examiners for evaluation. Based on the equational theory and local knowledge of the students ($A_i$) (Refer (24)), we propose the following inference system.

$$\frac{A_i \quad pk(B) \quad pk(X) \quad (QP_i, AS_{A_i}, pseudo_{A_i})}{aenc((QP_i, AS_{A_i}, pseudo_{A_i}), pk(B))}$$

Students at the end of the examination, submit the encrypted answer-books to the examination authority. Students may possess the knowledge of the examiners involved in the evaluation, but that knowledge is not sufficient to find the actual examiner involved in the evaluation of the particular answer-scripts. In other words, when two or more examiners are involved in the evaluation, examiner identity and the answer-script assigned to the examiner is indistinguishable to the student entity as indicated in the Eq. (28)

$$P[AS_{A_1}/x, X_1/y | AS_{A_2}/x, X_2/y] \approx P[AS_{A_1}/x, X_2/y | AS_{A_2}/x, X_1/y] \tag{28}$$

Thus, we can state that examination system with Remark! protocol provides *examiner anonymity before answer-script evaluation* from the student entity.

## 6 Conclusion

We, in this paper have defined a framework for modelling the examination system in the applied $\pi$ calculus to express the properties of associativity and anonymity. We investigated and modelled two existing examination systems, namely: conventional and electronic examination system using applied $\pi$ calculus and ProVerif. We defined series of associativity and anonymity properties

to analyze and validate the two examination systems. We proved that both the examination systems fail to provide the required level of associativity and anonymity between the question paper and answer-script exchanged between the examination authority and the students. As a future work, we, intend to study and compare/contrast the specific examination security requirements with those of other domains such as e-shopping and e-voting. Also, we plan to extend our work at the protocol level to detect plagiarism/collusion and student malpractices during the examination phases.

## References


1. Abadi, M., Fournet, C.: Mobile values, new names, and secure communication. ACM SIGPLAN Not. **36**(3), 104–115 (2001)
2. Apampa, K.M., Wills, G., Argles, D.: An approach to presence verification in summative e-assessment security. In: 2010 International Conference on Information Society (i-Society), pp. 647–651. IEEE (2010)
3. Bella, G., Giustolisi, R., Lenzini, G., Ryan, P.Y.A.: A secure exam protocol without trusted parties. In: Federrath, H., Gollmann, D. (eds.) SEC 2015. IAICT, vol. 455, pp. 495–509. Springer, Heidelberg (2015). doi:10.1007/978-3-319-18467-8_33
4. Bhardwaj, M., Singh, A.J.: Automated integrated examination system: a security concern. Inf. Secur. J. Glob. Perspect. **20**(3), 156–162 (2011)
5. Blanchet, B.: An efficient cryptographic protocol verifier based on prolog rules. In: Schneider, S. (ed.) 14th IEEE Computer Security Foundations Workshop, pp. 82–96. IEEE Computer Society Press (2001)
6. Blanchet, B., Abadi, M., Fournet, C.: Automated verification of selected equivalences for security protocols. In: 20th Annual IEEE Symposium on Logic in Computer Science (LICS 2005), pp. 331–340 (2005)
7. Castella-Roca, J., Herrera-Joancomarti, J., Dorca-Josa, A.: A secure e-exam management system. In: The First International Conference on Availability, Reliability and Security, ARES 2006. IEEE (2006)
8. Delaune, S., Kremer, S., Ryan, M.: Verifying privacy-type properties of electronic voting protocols. J. Comput. Secur. **17**(4), 435–487 (2009)
9. Dolev, D., Yao, A.C.: On the security of public key protocols. IEEE Trans. Inf. Theory **29**(2), 198–208 (1983)
10. Dreier, J., Giustolisi, R., Kassem, A., Lafourcade, P., Lenzini, G.: A framework for analyzing verifiability in traditional and electronic exams. In: Lopez, J., Wu, Y. (eds.) ISPEC 2015. LNCS, vol. 9065, pp. 514–529. Springer, Heidelberg (2015). doi:10.1007/978-3-319-17533-1_35
11. Dreier, J., Lafourcade, P., Lakhnech, Y.: Formal verification of e-auction protocols. In: Basin, D., Mitchell, J.C. (eds.) POST 2013. LNCS, vol. 7796, pp. 247–266. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36830-1_13
12. Eckstein, M.A.: Combating academic fraud: Towards a culture of integrity. International Institute for Educational Planning (2003)
13. Giustolisi, R., Lenzini, G., Bella, G.: What security for electronic exams? In: International Conference on Risks and Security of Internet and Systems (CRiSIS), pp. 1–5. IEEE (2013)
14. Giustolisi, R., Lenzini, G., Ryan, P.Y.A.: *Remark!*: a secure protocol for remote exams. In: Christianson, B., Malcolm, J., Matyáš, V., Švenda, P., Stajano, F., Anderson, J. (eds.) Security Protocols 2014. LNCS, vol. 8809, pp. 38–48. Springer, Heidelberg (2014). doi:10.1007/978-3-319-12400-1_5

15. Good, C.V., et al.: Dictionary of education (1945)
16. Huszti, A., Petho, A.: A secure electronic exam system. Publicationes Mathematicae Debrecen **77**(3–4), 299–312 (2010)
17. Kungpisdan, S.: Modelling, design, and analysis of secure mobile payment systems. Ph.D. thesis, Monash University (2005)
18. Maheshwari, V.: Malpractices in examinations-the termites destroying the educational set up (2011)
19. Morgan, C., O'reilly, M.: Assessing Open and Distance Learners. Psychology Press, Cambridge (1999)
20. Varble, D.: Reducing cheating opportunities in online test. Atlantic Mark. J. **3**(3), 9 (2014)