Towards reliable electronic exam networks

Jabbar El-Gburi

Doctoral Institute of Informatics,
University of Debrecen,
Debrecen, Hungary
Email: enjabbar.enjabbar@yahoo.com

Gautam Srivastava*

Department of Mathematics and Computer Science,
Brandon University,
Brandon, R7A 6A9, Canada
and
Research Center for Interneural Computing,
China Medical University,
Taichung 40402, Taiwan
Email: srivastavag@brandonu.ca
*Corresponding author

Senthilkumar Mohan

School of Information Technology and Engineering,
Vellore Institute of Technology,
Vellore, Tamilnadu, India
Email: senthilkumar.mohan@vit.ac.in

Abstract: In today's world, stable systems are what everyone is seeking. Furthermore, traits people desire in any system are trust, guarantees of security and fairness. Electronic exams should be considered as the hardest to defy to maintain trust in their relevance. Examination procedures concern any educational organisation which leads to various security techniques being utilised in order to maintain a minimum required level of security. In this paper, we present a secure e-exam network system that performs several processes such as evaluation, and management where all components are in a digital layout. We present a cryptographic platform that should be considered to obtain the required security standards of any educational institution for exam administering networks.

Keywords: cryptography; fairness; secrecy; security; e-learning; electronic exams security; networks.

Reference to this paper should be made as follows: El-Gburi, J., Srivastava, G. and Mohan, S. (2022) 'Towards reliable electronic exam networks', *Int. J. Computer Aided Engineering and Technology*, Vol. 16, No. 3, pp.344–361.

Biographical notes: Jabbar El-Gburi received his BSc in Electrical Engineering and Automation from the North University of China in 2000, Master's degree in Network Engineering from University of India in 2012. Currently, he is a PhD student at the University of Debrecen, Faculty of Informatics, Hungary.

Gautam Srivastava received his BSc degree from Briar Cliff University, USA in 2004, MSc and PhD degrees from the University of Victoria, Victoria, BC, Canada in 2006 and 2012, respectively. He then taught for three years at the Department of Computer Science, University of Victoria, where he was regarded as one of the top undergraduate professors in the computer science course instruction. From there in 2014, he joined a tenure-track position at Brandon University, Brandon, MB, Canada, where he is currently active in various professional and scholarly activities. He was promoted to the rank of Associate Professor, in 2018. He is active in research in the field of data mining and big data. In his eighth-year academic career, he has published a total of 90 papers in high-impact conferences in many countries and in high-status journals (SCI, SCIE).

Senthilkumar Mohan was felicitated with a PhD in Engineering and Technology from Vellore Institute of Technology in 2017. He obtained his MTech in IT from the VIT University in 2013. He earned his MS (SoftwareEng) degree in Computer Science and Engineering from VIT University Vellore, in 2007. He is presently working in the rank of Associate Professor at the Dept. of Software and System Engineering, Vellore Institute of Technology, School of Information Technology and Engineering, Vellore, India. His areas of research include artificial neural network, deep learning and cloud computing. He has contributed to many research articles in various journals and conferences of repute. He is also a member of a various professional society like CSI, Indian Congress, etc.

1 Introduction

With the increasing numbers in world population and extended demands on online learning, online exams have become an interesting topic in recent years. In this paper we develop a system that will allow a large number of students to take an exam in a secure environment to avoid cheating. We propose an anonymous return channel for exams to ensure a more secure mechanism of exams at a high level. Making an exam administered online saves cost and time with high security for exam providers. In addition, we apply an anonymous return channel among the participants of an electronic learning scheme, messages among the participants are anonymous, and teachers have to make sure that the students have to take the exam without talking to each other in the exam room that could be done by using surveillance cameras. This platform could be used by any education institution regardless of the number of students.

Our scheme is designed to do all types of exams like multiple choice, textual writing, and composition. After the students finish any given test, they have to submit the answers before the deadline of the exam. The exam organiser (EA) sends the papers to teachers to correct them and give final grades. This type of exam administration is very secure because the parties of the exam have no idea who wrote the test and this anonymity ensures that the students cannot contact the teacher and try to bribe him in order to get a good grade. After finishing the exam, students can get their grades and even those students who would like to upload their real data, the teachers still will not be able to see it. This paper explains our platform that can provide a highly secure protocol, based on cryptographic primitives. At the beginning of the academic year, each student has to register and get pseudonyms, which they receive via email.

We expand and correct some issues that were seen in Huszti and Pethő (2010). The main issue in Huszti and Pethő (2010) was that when a student complains against a specific teacher there was no mechanism to take any action against them. We introduce in the registration process a voting code, that when complaints are lodged against teachers, a given community can democratically vote against a given teacher to recover his encrypted data, so appropriate action may take place against them.

The rest of the paper is organised as follows. Section 2 introduces an overview of electronic exam learning. The proposed scheme is provided in Section 3. While Section 4 provides the security concepts of the exam scheme. We present some concluding remarks in Section 5.

2 Learning overview

Electronic exam management nowadays is a major pillar of any e-learning domain. Potentially electronic exams and instructors evaluation systems can induce additional security as a major part of the e-learning framework. Nevertheless, an e-exam model must fulfil all the distinctive attributes that conventional paper-based tests or long-established exams guarantee. It necessitates that the electronic approach should reduce obligations, preserve time and cost. Traditional exams offer the possibility to investigate student's identity and confirm it as well. The greatest challenge is to recognise each student and instructor. Our system presumes the presence of an e-exam centre that is monitored by an administrator, where all exam phases are accomplished electronically. Our proposed scheme assures anonymity of students and teachers as well. The teacher will not recognise student's identity as it is encrypted. A closer glance shows that the necessity for student's anonymity is dissimilar to teacher's anonymity. When the exam finishes students need to obtain their marks, for that reason we are concerned with retrieving their actual identity. To decide upon the manner to manage a secure e-exam, we define three types of entrants: teachers, students, and exam authority. The administration by the exam authority is to generate teacher profiles and to add or delete courses. Teacher's role is to provide course questions and displaying the assigned results. Finally, the student role is to initiate their own profile and also to take e-exams.

The proposed system paradigm considers a group of courses which are taught by teachers to registered students. Teachers that receive more than three electronic complaints will lead to a correction policy where voting process about the teacher will take place. We save the details of this for later in this paper.

Figure 1 displays the system flow diagram. Within this system, a user gets into the system, if they are a student then they will be asked to choose the course and the teacher to evaluate the teacher performance after receiving his grade, by filling and submitting an e-questionnaire. At this stage the system forwards this information to the exam authority, which in its part computes the impact to each teacher and sends it to the teacher's profile. Based on this profile the judgement on that teacher will be made by counting the threshold of more than three e-questionnaire generated complaints.

Figure 1 Representation of system model (see online version for colours)

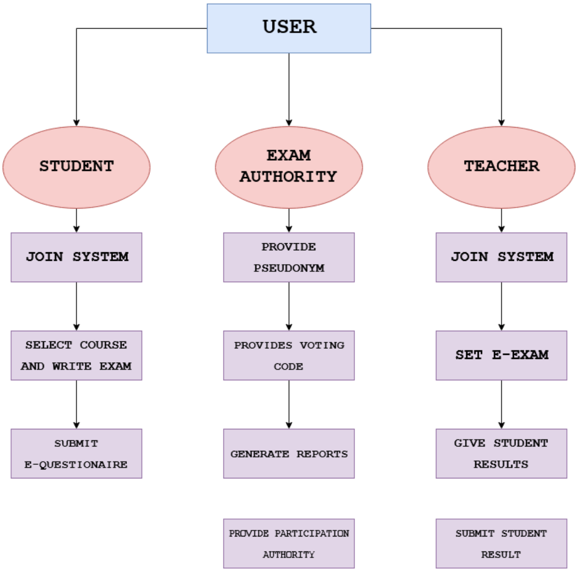
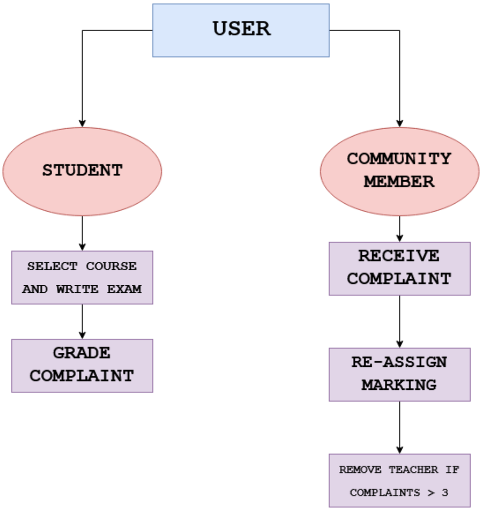


Figure 2 Summary of special case (see online version for colours)



In a special case when a student writes an exam and submits it. After a period of time the student will receive the result of that exam. If he is not satisfied with the grade that he received and thinks that they should receive a higher grade, then he has the ability to make a complaint through the system, so that his answers could be rechecked again. If the community members received more than three complaints against the same teacher then this teacher will be removed from the system and will lose the ability to be a member of the system as a teacher through a voting process performed by community members, these members are a small-scale of the exam authority members. Figure 2 shows an illustration of this special case.

2.1 Registration process

Students (S) and teachers (T) have to register at the beginning of the academic year, S to be able to write the exam and (T) to correct the test and send back the results to the EA. Moreover students can participate in any of the university activities like online classes, presentations, webinars, and lectures. Teachers (T) and students (S) get permission from the exam authority (EA) to do the exam. Students write the exam, teachers correct the exam and give the results. So, the students can see their result online after they sign in with their own private key. S_k is the secret key for the students and teachers, P_k is the public key for S and T, the questions are written by the community members C then they send it to the exam authority EA through an encrypted channel, server encrypted with El-Gamal algorithm. EA get the questions encrypted so that teachers cannot see them or do any change to the questions. The communication channel which is private gives the necessary opportunity for anonymous imparting or exchanging of information as in Golle and Jakobsson (2003).

2.2 Encrypted scheme

Registration process (R): in the registration time, each participant gets the public and secret key. R is trusted.

Teachers (T): correct the notes and give the result.

Students (S): write the exam and send the answers to EA.

Exam authority (EA): exam authority provides a pseudonym for the teachers, students, and provides code voting for the committee members to vote against any teacher. Gives the authority for only eligible students, teachers to participate in the exam based on their reports.

1 *Eligibility:* only eligible students can write the exam, EA can check if this student is eligible to write the test in this subject.

2 *Anonymity:* all the participating teachers, students and exam authority get a pseudonym in the registration period. All members are anonymous to each other. Students have no idea who is the teacher, teachers have no idea to whom this paper belongs to. EA he does not learn about the S, T, EA all members anonymous.

3 *Secrecy:* questions and answers stay secure in this scheme

4 *Test:* student is allowed to take the same exam only one time, after submitting the answer in this paper cannot be cancelled or ignored.

5 *Confirmation receipt:* after the student submit the test, he can get a confirmation letter proved to him that this test has been submitted successfully.

6 *Participants in our scheme:* the participant as flow, students (S), teachers (T), exam community (C), exam authority (EA).

2.3 Electronic learning scheme

We use public key cryptography, mainly El-Gamal algorithm, to generate the keys, encryption, and decryption, anonymous return channel between the participants. To register for the electronic exam, S and T get a pseudonym. This pseudonym is unique for each participants S and T. This pseudonym will be connected to the real data only after the exam ends. Students get their result after the EA recovers the real data of the student from the pseudonym, ends of the exam and then sends the result to the students. We use the equation

$$\begin{aligned} ExamScheme = (&Register_{S,T}, Ifeligibl_{S,T}, Writ, Exam, S, \\ &Correctpapers, T), geIDs) \end{aligned} \tag{1}$$

as given in Menezes et al. (1996), where

- Function $register(g_U; PK_U; SK_U; \bar{s}; randomvalue) \rightarrow$ pseudonym

  where g_U; PK_U, are participant's (student or teacher) public keying material and authenticates it with $\bar{s}$ private key of the exam and SK_U participant's private key. For each exam a new pseudonym is generated.

- Function $ifeligibl(pseudonym; subject) \rightarrow \{0; trans\}$

  Checks eligibility of the participant, i.e., whether the pseudonym is authorised for the subject given as input. The owner of the pseudonym is verified by running an interactive zero knowledge proof. It outputs transcript trans if it is correct and a 0 otherwise.

- Function $Writ(pseudonym; quest; answ; time) \rightarrow grade$

  Takes a pseudonym, questions, the answers and the duration time of the exam and outputs a grade.

- Function $geIds(pseudonym) \rightarrow identity$

  Takes a pseudonym and determine the corresponding real identity of the student, in order to give his/her grade.

At the exam, the students and teachers must register in the database of the university and get a pseudonym (Huszti and Pethő, 2010). This pseudonym programmed to give the ability for the EA to recover the identity of the S only ends of the exam to send the grade to them, and what is his eligibility in the exam time. If he is a student, he can take the exam or if he is a teacher he can correct the papers and give the result, before sending the questions to the students and the answers to the teacher, EA can check if they are authorised for this exam, moreover exam authority check if this student his first time taking the test.

2.4 El-Gamal cryptosystem algorithm

El-Gamal encryption is an asymmetric encryption algorithm; it is public key cryptography based on DH key exchange. The one-way function that gives us the encryption and the decryption, running in separate function, using public key cryptosystem. P, Q are huge prime numbers. El-Gamal is semantically secure under the Diffie-Hellman (DH) assumption, El-Gamal solved the main problem with DH, with key exchange algorithm, proposing random exponent type key. The receiver has to generate the key and publish it. El-Gamal encryption uses asymmetric encryption. Steps of this algorithm are key generator, encryption and decryption algorithm. This is public key encryption made up from three algorithms: Gen algorithm, it is a generator algorithm that generates a public key and secret key; encrypt and decrypt algorithms. Encryption algorithm encrypts using a public key and decryption algorithm decrypt using a secret key. We do not use a fixed generator because it allows us somewhat to use a weaker assumption improving security, it is better to choose a random generator every time. It is easy to do that by taking the generator that we started with, then we raise it to some power that relatively prime to n, that would give us another generator of the group G.

Alice chooses some number r and computes $K_a \equiv a^r mod\ N.$

Bob chooses some number s and computes $K_b \equiv a^s mod\ N.$

Alice and Bob exchange K_a, K_b.

Alice computes $K_b^r$and Bob computes K_a^s. Note they both have a^{rs} mod N, but neither r nor s has been transmitted. This method of exchanging mod N is called Diffie-Hillman key exchange protocol.

Bob computes p as $c \equiv$ a^{rs} p mod N, Alice decrypts using $p \equiv$ (a^{rs})$^{-1}$ mod N. Example, encrypt and decrypt $p = 35$ using base $a = 5$ and modulus $N = 89$, now Bob and Alice choose a random number, Bob chooses $r = 8$, and Alice chooses $s = 13$, then they chose random numbers both of them (Grewal, 2015).

2.5 Registration scheme

Step 1 Registration $(g_r, P_{kr}, S_{kr}, S^-, (c', e', d', C)$, random number) (Folláth, 2010). Pseudonym P_k, S_k are public, and private keys respectively. S^- is the secret key for each subject, each subject has the different secret key, (c', e', d') is the voting code for the community members to vote against any teacher. g_r is the participant registration public key and its authenticated with S^-, a random number is the identification number for the participant-generated randomly EA gives the authority for an only eligible student, random number for the student's identification.

Step 2 If eligible (pseudonym, exam types) → (0, accept)

If this student is allowed to take the exam in this subject, give conform with receipt-free after submission, or else 0

Step 3 Write the exam (pseudonym, questions, answer, time). Result Login to the exam system with personal Pseudonym, get questions, give answers in chosen time for that exam, submit the answers and get the result after.

Step 4 `EA getIDs(pseudonym)` → name of the student. Exam authority gets the identification of the student from the pseudonym of the student after the exam period; send the grades to the server for the students to get them online. Information security can be seen as an approach that depicts all the plans or course of action taken to achieve the prohibition of unsanctioned utilisation of electronic data, if this unauthorised utilisation converts to a shape of impairment, releasing secret information, or perturbation. Moreover, cryptography and the aspect of protecting the information have a mutual sense of preserve the privacy, integrity, and accessibility of the information disregarding the data that originate from documents either the printed or the electronic one. Cryptography is considered as the greatest crucial domain of data security (Menezes et al., 1996).

We give a technique of conveying private data over a network which is open (refer to Figure 3). Nevertheless, cryptography offers several services like privacy, authentication, secrecy, and availability. The robustness also the length of the cryptographic key is believed to be a prime method. The keys which are utilised for the purpose of encryption and decryption should be powerful to the required degree or extent in order to generate vigorous encryption. Thus they ought to be kept safe from unauthorised access and should be obtainable when needed. Cryptography as well contributes to information technology, essentially in the approach that is utilised in security scope for access control, privacy, and confidentiality (Branovic et al., 2003). It is also utilised in several applications that come across daily actions like electronic commerce, server password, and electronic voting.

Figure 3 Cryptographic platform for registration process (see online version for colours)

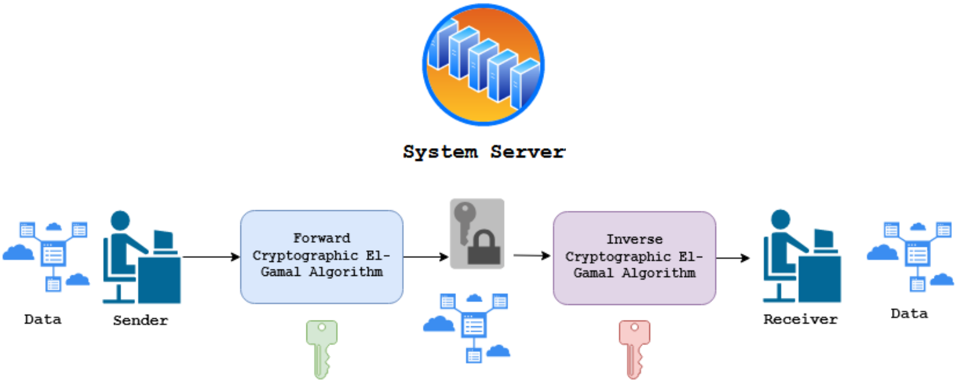

System Server
Data
Sender
Forward Cryptographic El-Gamal Algorithm
Inverse Cryptographic El-Gamal Algorithm
Receiver
Data

Figure 4 Identification phase process (see online version for colours)

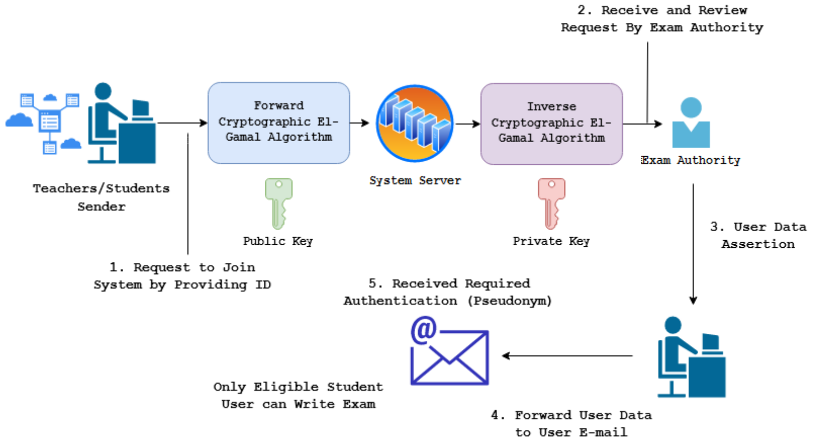
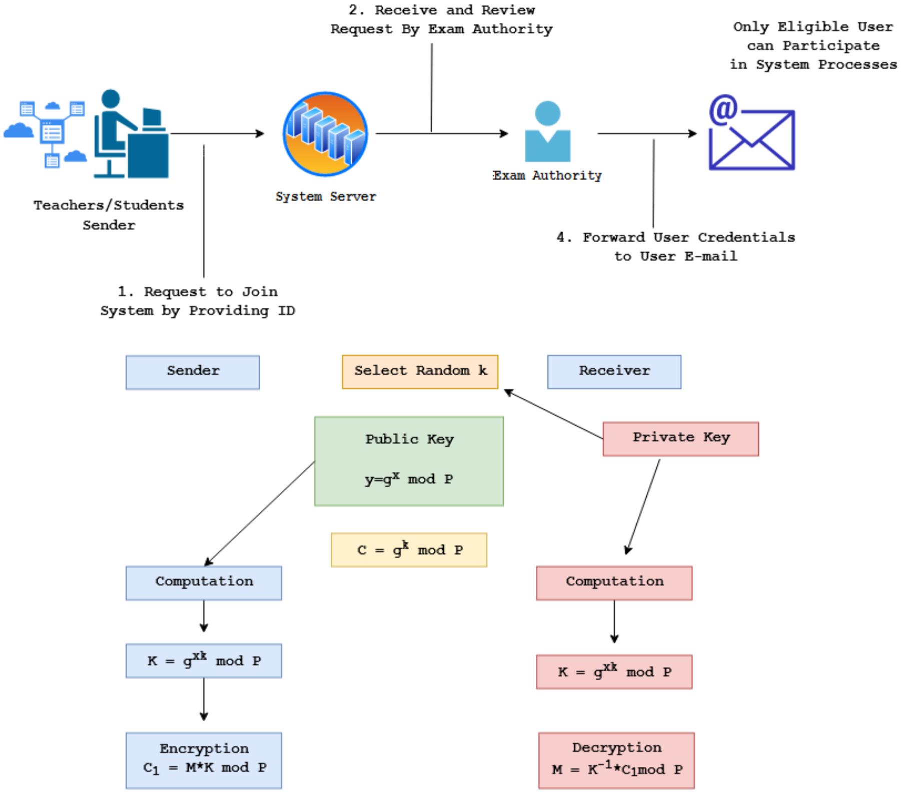

2. Receive and Review Request By Exam Authority
Teachers/Students Sender
Forward Cryptographic El-Gamal Algorithm
Public Key
System Server
Inverse Cryptographic El-Gamal Algorithm
Private Key
Exam Authority
3. User Data Assertion
1. Request to Join System by Providing ID
5. Received Required Authentication (Pseudonym)
Only Eligible Student User can Write Exam
4. Forward User Data to User E-mail

Figure 5 Authentication phase process (see online version for colours)



The process of authentication and identification is utilised to recognise or indicate who wants to establish a connection also to validate any entity that operates on the existed system, the identification phase can be considered as a part of the registration process, this is where we could verify if the user has the right to participate in any system process, also for specific users they can acquire the ability to vote against a teacher who received more than three complaints. Once the user has registered in the system, the below steps will be fulfilled, as illustrated in Figure 4, the user turns into an authenticated user, either as a student or a teacher after phase number 2. While in the third and fourth phases, the users data will be protected and saved in the system server and will be copied also and forwarded to the user personal email.

While the authentication phase takes place instantly before the process of taking the exam or voting, in these phases the user can participate in the related processes by providing his credentials, the authentication process is elucidated in Figure 5, since the start till the end, the system users login to the system website via using his credentials and the provided public keys. Once the user has signed to the system, the system server will create a computed `El-Gamal` public-key, this key will be passed to the user email when it is used the system user will be ready to continue and participate in the system processes.

Participants can communicate anonymously, students (`S`), teachers (`T`) and exam authority (`EA`) can exchange several anonymous messages without revealing the real data for the sender and the receiver. This channel is re-encrypt the message using mix networks based on the `El-Gamal` encryption algorithm, allowed to re-encrypt the Ciphertexts. Servers generate public and private keys based on `El-Gamal` encryption algorithm, the public key went publicly for everyone G_q, g, pk, the secret key S_k shared between the Mixnet servers and this server share a signing key for the participant.

Step 1 To send a message between Alice and Bob they have to be identified, an identification key and public key for Alice, Bob key

$$Enc_{Mix}(IDA||PkA), Enc_{Mix}(M), Enc_{Mix}(IDB||PkB)) \tag{2}$$

as given in Castella-Roca et al. (2006).

Step 2 Mix and re-encrypt the message

Servers mix and re-encrypt N of messages, with keeping these messages in orders.

Step 3 Deliver the messages

The mix-net server encrypts the message Enc_{Mix}(M), to $EncPk_B$(M) generate signing up on Enc_{Mix}(ID$_A$//Pk$_A$). B receives $Enc_{Mix}(ID_A||Pk_A)$, Sig, $EncPk_B$(M)).

Step 4 Forwarding the message

The receiver would like to reply X to the A then it will submit it to the Mixnet server ($Enc_{Mix}(ID_A||Pk_A)Enc_{Mix}$(X), $Enc_{Mix}(ID_A||Pk_A)$, Sig.

Step 5 Timed-release service

We use `TSA` to get back the student's identity to send them the grades after the exam ends. Our network containing several servers to mix and re-encrypt

> the messages using RSA algorithm, in the registration time, using Q and P as prime number, Q(P - 1) $G_{Q,}$ the NET get the message as input g_r(mod p) to calculate the output g_r^L(mod p) L is the secret key. The cryptosystem of public-key aspect relies on the public-key scheme which is exploited by the sender side to encrypt the sent information, the second key is recognised as the private key, which is exploited to decrypt the encrypted data that has arrived at the receiver side, so it is a private key that belongs to the receiver.

There exist several algorithms for public-key encryption and digital signatures, however, a small number of them are mutually functionally effective and secure such as ElGamal (El Gamal, 1985). Singh and Kumar (2012) are other researchers who characterised this algorithm.

3 Proposed scheme

Exam authority (EA) can arrange more than one exam at the same time, for each subject, there are several teachers to do the correction and the teacher can correct papers in more than one subjects. All the teachers and students having a digital certificate, all the participant have secret key this key kept secret with the user to prevent the attackers.

During the registration time, R generates all the participant's requirements generate public, private keys, chose P, Q large prime numbers $Q(P-1)$. G_Q Multiplicative sub-group of order, each member in this scheme chooses randomly a secret key $\mathrm{Sk}_r \in ZQ$ and random number $g_r \in G_Q$. Calculates $PK_, \equiv gr^{skr}r$ (mod P), this is information publicly shared, public and secret keys used in many exams. Online information's published about the student, his public key and if he is an eligible student and allowed to take this exam (gs, Pk_Q), before every exam EA chose the secret key for the subject and the allowed student then exam authority publish the exam publicly for the student to be able to write the exam in the exam time. $S^- \in Z_Q$, $g^- \in G_q$ information about the exam as flowing, (g^-, h^-) where $h^- \equiv g^-$ (mod P) and keeps S^- secret. Each server gets the El-Gamal keys. In this exam scheme community members to generate the questions, let, Pk_C, Sk_C public, and secret keys respectively, exam questions are sent encrypted by Mixnet server, questions are issued by the C authentication signature, exam authority receive

$$Enc_{Mix}(quest||SigC(quest||time1)), \tag{3}$$

as given in El Gamal (1985).

These questions are encrypted, EA cannot see them nor do any change, Sig_C is the certificate of the authority for the community members, Time1 is the starting time for the exam.

3.1 Registration process

Registration phase using ElGamal algorithm.

1 Users (can be teachers or students) have to register at the beginning of the academic year.

2 Eligibility of the users is checked by the exam authority. If students are eligible to write the exam or not and teacher are eligible to check papers or not.

3 After successful registration users and with the help of their public and private keys the pseudonym will be generated. Where P^- is a pseudonym, pk_r is a public key, S^- and g^- is information about exam, P large prime number

$$P^- \equiv pk_r S^- (\text{mod P}) \tag{4}$$

4 If user is eligible student do

a exam authority, server: (P^-, g^-)

b server: calculates $P' \equiv P^-$ (mod P) and $r \equiv g_r$ (mod P) each server have encrypted secure ((time, y_i, P^-, g_r)) time that is the time when g_r can be published an (y_i) is the shared secret key .

c server, user: (r, P')

Else

a exam authority, user: (P^-, g_u)

b U: Calculate $P' \equiv P^-$ (mod P) and $r \equiv P^a$ (mod P), where a is randomly chosen

End if

U : calculate $P \equiv r^{asr}$ (mod P).

U, EA: EA gives the authority for the S and T to participate in the exam, U as a verifier runs an interactive zero-knowledge proof of the equality of discrete logarithms of (P, P^-), (g^-, h^-) ends of the registration time, users process (r, p, P'). Eligible students pseudonym is (a, b, b'), and teachers pseudonym is (e, f, f') for the teachers there is no time release service. We do not need to connect their real data to the online database, for the students we have to connect it to the student can get his result after the ends of the exam. Student can use his secret key to log in and see his result online.

3.2 Examination process

exam authority check eligibility of the students S and teachers T, if eligible of the student (a, b, b') if he is allowed to take the exam in this subject, and teachers if eligible (e, f, f') if that teacher eligible to correct the papers in this subject and give the grades,

1 Student: check the message $M = (a||b||b')$ subject

Student applies to the EA to get the authority and write the exam in the exam time

Student → exam authority: student submits

$$(Enc_{Mix}(ID_s||Pk_s)Enc_{Mix}(M)(Enc_{Mix}(ID_{EA}||Pk_{EA})(M) \tag{5}$$

ID_s Identification number of the student, PK_s is the public key for the student, ID_{EA} is the identification number of the exam authority, PK_{EA} is the public key for the exam authority, each server in this scheme mix and re-encrypt set of message using `El-Gamal` encryption algorithm, after sending the message to the exam authority,

Exam authority gets the message as flow

$$(Enc_{Mix}(ID_s||Pk_s), sig_{mix}(ID_s||Pk_s),\ (EncPk_{EA}(M)) \tag{6}$$

Public and secret key of the students generated by the server using `El-Gamal` algorithm

2 T send message to the exam authority in the same way using his pseudonym $M = (e, f, f')$,

3 EA after receiving the message from the student or teacher, EA check is this pseudonym is it authorised for the student and or the teachers,

$((b^{s-} \equiv b'(\text{mod } P) \text{ or } f^{s-} \equiv f'),$

`EA` run zero knowledge (`ZK`) for the proof knowledge of the secret key, encrypted with the server public key,

$$((\text{a, b, b}), Trans_T, (e, f, f'); Trans_T, Enc_{mix}(ID_T||Pk_T), \text{subject}) \tag{7}$$

Pseudonym and transcript of the students and teachers,

4 Exam authority → student: exam authority send back the questions in an anonymous return channel, `EA` send the messages to the server to mix the message and re-encrypt them,

$$(Enc_{mix}(ID_{EA}||Pk_{EA})Enc_{mix}(M, Enc_{mix}(ID_s||Pk_s), sig_{mix}(ID_s||Pk_s)) \tag{8}$$

where $M =$ question $S||sig_c$(question S)||time.

sig_c is the exam questions written and sign by the community members of the exam.

5 Exam authority → student: students answer the questions and send them back to the `EA`, in a chosen time for that exam,

$$M = a//b||Enc_{mix}(\text{answer S})||\text{time2} \tag{9}$$

6 Exam authority → student: `EA` store encrypted questions (Questions, time1, time2, Enc_{mix}((answ)), student receive hash function of all the encrypted data, prove for the submission exam.

7 `EA`: exam authority chose for each exam teacher do the correction and send back the grades to the `EA`,

$$(Enc_{mix}(ID_{EA}||Pk_{EA}),\ Enc_{mix}(\text{answer S}),\ Enc_{mix}(ID_T||Pk_T)). \tag{10}$$

8 Teacher → exam authority: `T` teachers correct the test, give the result, and send them back to the `EA`

M = (result||Hash (result//answer S)|| [Hash (result||answer S)] SK_T || noninter),

noninter is the non-interactive knowledge `ZK` zero knowledge (Srivastava et al., 2018b).

3.3 Rating process

1 Exam authority will provide the ratings (c, e, d') for community members and community members C Before distributing the code, exam authority sends it to the server, this server mix the code and re-encrypt it, then distribute it to the community members in an anonymous return channel

$$(Enc_{mix}(ID_{EA}||Pk_{EA}),\ Enc_{mix}(\text{code}),\ Enc_{mix}(ID_C||Pk_C)) \tag{11}$$

After distribution, EA got a proof message that the distribution is done successfully.

2 C sign against one teacher, $Enc_{mix}(ID_C||Pk_C), Enc_{mix}(c, e, d'); Enc_{mix}(e,f,f')$.

3 Using the code to sign against this pseudonym of the $T(e, f, f')$ to recover his real identity.

4 EA can get the identity of the teacher after the message arrive from the community, that this teacher has been removed, the majority of the community has signed against him, then EA can recover the real identity of the teacher ID_C, Pk_C is the community secret and public keys, ID_T, Pk_T, is the secret and public keys respectively of the teachers (Srivastava et al., 2018a).

3.4 Exam members

Students are active in the database with public and private key. Students apply to take the exam with their pseudonym (a,b,b'), exam authority (EA). Check if this student S allowed to take the exam, moreover teacher T have to register in the database of the university to be able to correct the papers after the exam time. EA have to check the eligibility of the teacher by checking the pseudonym of the teacher before giving the authority to correct the papers and give the grades (e, f, f'). Students run function of (write exam, questions, answers, time)

$$(Enc_{mix}(ID_S||Pk_S),\ Enc_{mix}(\text{M}),\ Enc_{mix}(ID_{EA}||Pk_{EA})) \tag{12}$$

where ID_s are the identification of the student S created randomly; Pk is the public key of the student S. Students can use different identification number for each message, the server collects a batch of messages mix them and re-encrypt them in a chosen period of time using El-Gamal encryption algorithm after that server gives proof of mixing the message and send them to the exam authority. EA can check if this pseudonym is authorised student, teacher or not, by checking the congruence $b^s \equiv b'$ (mod P) or $f^s \equiv f'$ (mod P) and check if this S did this exam before or not, S^- is the secret exponent of the subject. Teacher T after correcting the papers he can give the result and send it back to the exam authority with an anonymous return channel. EA will not see the result either the name of the student, this result will be published online and only the student can sign and see his/her result. To get authenticate for the exam from the exam authority, students and teachers have to apply with their pseudonym, exam authority make sure if this is the owner of this pseudonym by running ZK proof, zero-knowledge proof in case of a student(a, b) and teachers(e, f) (Dwivedi and Srivastava, 2018).

Here, we show

$$Enc_{Mix}(ID_A||PK_A),\ Enc_{Mix}(M),\ Enc_{Mix}(ID_B||PK_B)) \tag{13}$$

where ID_A is the private key of the sender, PK_A is the public key of the sender, M is the message, ID_B, PK_B is the privet and public key respectively for the receiver.

4 Exam scheme security

The selected students who take the exam are authenticated by the exam authority. The authorised exam has to make sure that the registered student will not ask another one to take the exam on behalf of them. Authenticity avoids this attack. The exam takers have to be sure this is the valid exam questions by the selected members of the faculty. It has to be clear that this grade has been written by only selected teachers and this teacher have to be authorised and registered in our database, so they can have the authority to do the correction in the exam time.

Exam takers sometimes are known to bribe the teachers in order to have good marks. This is why in this scheme students will have no idea who is correcting their papers and the teachers have no idea to whom the exams belong. Teachers can log in and start the process without using their real personal data. This means all the data will be encrypted for all of the participants, students, and teachers in this process.

The key steps taken during the exam are described as follows:

- *Robustness:* questions in the exam cannot be changed and the submitted exam cannot be ignored.
- *Correctness:* the students who took the test already cannot take it once more. After sending the exam papers to the EA, it cannot be denied because it is already submitted and it cannot be cancelled.
- *Conformation:* after the students finishing writing the test and submitted the answers, they can get an automatic reply that their submission successfully conforms. The registered in this scheme are the exam authority, teachers and the students. During the registration, each of them gets two keys one has to secret key and the second key will be a public key it will be published (Dwivedi and Srivastava, 2018). Registry R during the registration at the beginning of the academic year in the university all the participant has to register and get secret and public keys. Students and teachers responsible to keep this key secrete to keep this student able to log in and do the exam request in the time of the test, Students S who would like to do the test might be attacker, the EA has to check before giving the authority to the student to write the exam. Exam authority EA gives pseudonyms for eligible people, supports the whole procedure during the exam, chooses teachers for the students after the exam submitted to give the grade. The procedure of the exam scheme using public key cryptography, mainly El-Gamal encryption based on the Diffie-Hellman key exchange protocol. The semester starts with the registration time, students and teachers have to get the pseudonym, and this will be unique for everyone, it is totally separated for each S and T and they cannot communicate with each other. All the students and teachers

> get pseudonym in the registration time, it is special for each participant, they can log in with. Student can get a new key for each new exam, this generated from the master key that the EA can recognise. With the request of the student to take the exam, EA can check if this is already an authorised student and he is allowed to take the exam. After writing the test student have to submit their answer and wait for the grade. The EA have to check if this student is allowed to take the exam or not, if yes, then he can send the questions papers to the responsible teach to correct them. The teacher can send back the grade, EA after getting the papers have been corrected and get the grade then the EA can send them to the students and only that specific student can see that grade.

If the student is allowed to take the exam and he has an active pseudonym for the exam, then he can log in with his details and write the exam if the student logged in with his real data the pseudonym will give 1 or else 0 instead (Dwivedi et al., 2019b).

Writing the exam: (Pseudonym, Questions, Answer, Time)-Grade, all this will be input, and the output will be the grades. Depending on the Pseudonym of the participant, EA can get S's identity and give the grades.

During registration, EA distributes the code(c, e, d') randomly between the community members C of the exam, in the university. Before distributing the code, exam authority sends it to the Mixnet server, this server mixes the code and re-encrypt it, then distribute it to the community members in an anonymous return channel. This code can be used several times to distribute the code from (EA to C)

$$Enc_{Mix}(ID_{EA}||Pk_{EA}), Enc_{Mix}(Code), Enc_{Mix}(ID_C||PK_C)) \tag{14}$$

ID_C, PK_C is the secret and public ID respectively of the community members, Enc$_{Mix}$(Code) is the distributed code to the community, to vote against the chosen teacher, to take off the authority of being able to correct the papers for the students. Enc$_{Mix}$(ID$_{EA}||PK_{EA}$) is the secret and public key of the exam authority. Public key generated by the servers that connected to each other's using El-Gamal cryptosystem, gq, g, P_k, published, the secret key is shared with the mixnet servers, these servers share a signing key. Now there are two keys public the one shared publicly and the privet key for the users to sign against any teacher, this code created by the El-Gamal encryption algorithm. One of the most important features kept this algorithm between the strongest encryption algorithms that it can create the code, encrypt and decrypt the message (G, e, d).

Community members get the message after it is re-encrypted by the Mixnet servers, then C get the message as flow $Enc_{Mix}(ID_{EA}||Pk_{EA})$,$Sig$,$Enc_{PkC}$(M)). This message includes a signature for the community with the Pk of the community to prevent the middle attach of having the code and use it in a threatening way against the teachers. Then EA destroys the code after distributing it to all members for security reason, now each member has a code. Only all or most of the members sign with their code against one teacher, then this teacher can be removed from the pool of the teachers who are allowed to correct seminar works. After distribution, EA got a proof message that the distribution is done successfully.

C sign against one teacher, $Enc_{Mix}(ID_C//PK_C)$,Enc_{Mix},(c, e, d'); $Enc_{Mix}(e, f, f')$. Using the code to sign against this pseudonym of the T (e,f,f') to recover his real identity EA can get the identity of the teacher after the message arrives from the community. The teacher has been removed, the majority of the community has signed against him, then EA can recover the real identity of the teacher ID_c, PK_c is the community secret and public keys, ID_T, Pk_T, is the secret and public keys respectively of the teachers. Creating randomly all the student's numbers and re-encrypt it (Dwivedi et al., 2019a). Exam authority, before giving the authority to the students that requests for the exam, have to see if this student allowed to take this exam and this subject the one he applied for, to do the test in, then he will be allowed to write the test and send it in given time for that exam. The EA reply the request without knowing exactly the real name of these students, he only can see the random number so EA can reply that with return channel, reply with the authority to do the exam besides the actual time of that test. Teachers can comment after exam time. When the students have any questions at the end of the exam and after getting the grade, they still can send their questions and submitted in that secure channel Mix net. The teacher can write back without knowing who is this student only to reply to the questions if there is any, that also can be an agreed time only after the exam ended.

Public key encryption application example like secure email, Bob has Alice's public key and sends her an email, Encrypted file system, Bob want to store the encrypted file in storage server E(K_f, File) send it to Alice. Alice can access this file after she is back even after bob he is offline after sending the message he can leave this message encrypted and only Alice can decrepit this message because it encrypted by using her public key,

E(Pk_A, K_f), E(Pk_B, K_f)-Key escrow, data recovery without Bob's key, E (K_f, File), E(Pk escrow, K_f), E(Pk_B, K_f), Bob write to the data server with escrow authority in case bob in a sick leave or fired still the company can access this files and use it after bob has gone away from this company, not to lose these files. The voting process usually is quite censorious; as the voter user is not able to logout of the system after being given the public key. In spite of that, the voters (community members) to retrieve and identify the teacher that they are going to vote against, after it is re-encrypted by the Mixnet servers, in order to be removed from the system.

5 Conclusions

This paper demonstrates the scope of establishing a reliable protocol founded on the cryptosystem of public-key encryption. The proposed scheme covers all the security required for an e-learning system with authenticity, fairness, and secrecy, without using a trusted third party. The system can be used to create examinations among students, by using secure and easy e-learning methods. The El-Gamal cryptosystem algorithm and protocol proposed are meant to make exams secure and safe. Encryption and decryption will also make sure information is secure and confidential for both students and teachers. The proposed system saves time and information can be assured has a higher amount of security.

References

Branovic, I., Giorgi, R. and Martinelli, E. (2003) 'Memory performance of public-key cryptography methods in mobile environments', *ACM SIGARCH Workshop on Memory Performance: Dealing with Applications, Systems and Architecture (MEDEA-03)*, New Orleans, LA, USA, pp.24–31.

Castella-Roca, J., Herrera-Joancomarti, J. and Dorca-Josa, A. (2006) 'A secure e-exam management system', *Proceedings of the First International Conference on Availability, Reliability and Security (ARES '06)*, pp.864–871, IEEE Computer Society, Washington, DC, USA [online] http://dx.doi.org/10.1109/ARES.2006.14.

Dwivedi, A.D. and Srivastava, G. (2018) 'Differential cryptanalysis of round-reduced LEA', *IEEE Access*, Vol. 6, pp.79105–79113.

Dwivedi, A.D., Dhar, S., Srivastava, G. and Singh, R. (2019a) 'Cryptanalysis of round-reduced Fantomas, Robin and iSCREAM', *Cryptography*, Vol. 3, No. 1, p.4.

Dwivedi, A.D., Morawiecki, P. and Srivastava, G. (2019b) 'Differential cryptanalysis of round-reduced speck suitable for internet of things devices', *IEEE Access*, Vol. 7, pp.16476–16486.

El Gamal, T. (1985) 'A public key cryptosystem and a signature scheme based on discrete logarithms', in Blakley, G.R. and Chaum, D. (Eds.): *Proceedings of CRYPTO 84 on Advances in Cryptology*, pp.10–18, Springer-Verlag New York, Inc., New York, NY, USA.

Folláth, J. (2010) 'Construction of pseudorandom binary sequences using additive characters', *Period. Math. Hung.*, Vol. 60, No. 2, p.127.

Golle, P. and Jakobsson, M. (2003) 'Reusable anonymous return channels', *Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society (WPES '03)*, pp.94–100, ACM, New York, NY, USA [online] http://dx.doi.org/10.1145/1005140.1005155.

Grewal, J.K. (2015) *ElGamal: Public-Key Cryptosystem*, A paper presented for the degree of Master of Science, Math and Computer Science Department, Indiana State University.

Huszti, A. and Pethő, A. (2010) 'A secure electronic exam system', *Publicationes Mathematicae*, Vol. 77, Nos. 3–4, pp.299–312.

Menezes, A., van Oorschot, P. and Vanstone, S. (1996) *Handbook of Applied Cryptography*, pp.4–15, CRC Press, 516pp.

Singh, R. and Kumar, S. (2012) 'Elgamal's algorithm in cryptography', *International Journal of Scientific & Engineering Research*, Vol. 3, No. 12, pp.1–4.

Srivastava, G., Dwivedi, A.D. and Singh, R. (2018a) 'Crypto-democracy: a decentralized voting scheme using blockchain technology', *ICETE*, July, Vol. 2, pp.674–679.

Srivastava, G., Dwivedi, A.D. and Singh, R. (2018b) 'PHANTOM protocol as the new crypto-democracy', *IFIP International Conference on Computer Information Systems and Industrial Management*, September, pp.499–509, Springer, Cham.