Data Storage of Electronic Exams

Lütfü Tarkan Ölçüoğlu, Sedat Akleylek

***Abstract*—Electronic learning is one of the most popular topics of today's technology and education. The development in technology forces universities, colleges and other education institutes to transfer their materials into digitized environment. Moreover, this new education system allows students to attend lessons from their computers located out of campus. In fact, some of the universities and colleges have started to hold their examinations in electronic environment. Electronic exam is one of the hardest problems in electronic learning subject, since it needs authenticity, anonymity, robustness and secrecy for all parts. The secrecy of electronic exam depends on the secrecy of both questions and their answers. In this work, we propose a data storage model for electronic exam which provides a long term confidentiality on the sensitive data such as questions and their corresponding answers by using verifiable secret sharing scheme.**

***Index Terms*—Long term confidentiality, verifiable secret sharing scheme, threshold cryptography, e-learning, e-exam.**

I. Introduction

THE development in technology affects every part of our life. People need to reach any data in a quick way, so that almost every data in any field have started to become digital and stored in database servers. For instant access to data, lots of institutions started to store their data in cloud systems. Some of this data in cloud has secret information and should be stored in encrypted form. Unfortunately, the encrypted form of secret information in cloud does not provide full secrecy since the encryption algorithm is not resistant forever. Therefore, new storage techniques are needed to provide full secrecy.

Education is one of the crucial parts of our life and there have been enormous technological developments in this area. Over two decades, lots of institutes, universities, colleges have transferred their documents to computerized environment especially to cloud which provides instant access to materials for both students and teachers. These developments in education have revealed a new definition to literature: electronic learning (e-learning). The first definition of e-learning was done in 1999 during CBT system seminar in Los Angeles. However, the development in e-learning field enabled lots of universities, colleges and institutes to hold their exams in a computerized environment. Electronic examination (e-exam) is one of the difficult parts of e-learning since there have been great amount of sensitive data behind it. Basically, e-exam can be defined as the computerized version of paper based exam on the other hand, for holding a secure electronic exam, there are cryptographic problems to be solved. Furthermore, an e-exam consists of registration, question preparation, exam preparation, evaluation and archiving parts. In registration part, students are registered for the exam and some relevant information are taken. Questions and answers are prepared by question makers and sent to authority in question preparation part. The authority prepares exam and after examination both evaluation and archiving processes are performed. These phases can be achieved by using cryptographic techniques due to satisfying information security concepts. The security of e-exam relies on the secrecy of questions and answers. The most popular example of electronic exam is the test of English as a foreign language (TOEFL) by educational testing service (ETS) [12]. More than 30 million people [11] have taken the test all over the world. The structure of TOEFL is mainly based on creating and administering the test questions, analysing the results, rejecting or revising the questions and releasing the test questions in a test form phases. They use the Internet security protocols which is used by major financial companies for transmission of the exam questions. The exam questions are downloaded to client's computer in encrypted form. Not only TOEFL, but also other popular electronic examinations like graduate record examination (GRE) and graduate management admission test (GMAT) use the same security protocols but the details of them are not revealed. One of the detailed work in this area was done by Jordi et al., [6] who proposed an e-exam scheme divided into stages: setting up an exam, beginning, holding and submitting of the exam, grading of exam, obtaining the score of the exam answer and revising of exam. They identified the security requirements for electronic exam as authenticity, privacy, correction, secrecy, receipt and copy detection. In this scheme, the privacy was achieved by the maximum impartiality, i.e., the teachers should not know the identity of the students while grading the exam. On the other hand, exam questions were kept in secret and the secrecy of the questions and answers was achieved by the encryption with manager's public key since all participants have digital certificates. Exam questions were prepared by teachers and they were encrypted with manager's public key. The storage of sensitive data was done just only encryption with manager's public key. In [2] Huszti and Pethö's proposed electronic examination scheme, they emphasized the secrecy of student's identity. The exam scheme consists of registration, exam and grading phases. The anonymity of students' identities provided by timed-release service containing n-servers. The secret, i.e., the identity of students shared into other servers by Shamir's secret sharing system. They proposed to use Mixnet for data storage. The questions were created by a committee and they were encrypted with Mixnet's public key. The authenticity of the questions was assured by committee's signatures. Both [6] and [2] emphasize the secrecy of the identity of students and in both scheme, the exam questions are prepared, encrypted

Lütfü Tarkan Ölçüoğlu is with the Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey (e156792@metu.edu.tr)

Sedat Akleylek is with the Department of Computer Engineering, Ondokuz Mayis University, Samsun, Turkey (sedat.akleylek@bil.omu.edu.tr).

and used in the exam, so that there is no long term storage for exam questions.

A. Our Contribution

Our aim in this work is to propose a data storage protocol for secure electronic exam consisting of secret sharing and long term confidentiality on sensitive data. The long term confidentiality of sensitive data is one the biggest challenges and practical long term confidentiality is an open problem. Since the secrecy of e-exam depends on the secrecy of questions and answers, the data storage of such sensitive data is important. Other related works [6] and [2] emphasized the secrecy of the students' identity and both of them encrypted questions and answers with authority's or Mixnet's public key. Single encryption of such sensitive data is not enough, so that long term confidentiality issues should be thought. Unlike [6] and [2], our model emphasizes the long term confidentiality of the sensitive data.

B. Roadmap

The outline of the paper is as follows: In section II, we give some brief information about cryptographic needs and definitions. In section III, the data storage model is defined in details. The security analysis of the model is done in section IV. Finally, in section V, the conclusion and future work are given.

II. PRELIMINARIES

In this section we give some definitions and brief information about cryptographic requirements. The algorithms and protocols defined in this section will be used in the model. The security requirement of the given model based on symmetric cipher for the encryption of the question and answers, asymmetric key encryption for authentication issues and threshold cryptography for long term confidentiality to provide confidentiality.

A. Symmetric Key Encryption: AES

AES is used for confidentiality of our questions' main parts. The AES [7] also known as Rijndael was developed by Vincent Rijmen and Joan Daemen in 2001. It was the winner of AES competition established by NIST. AES is a substitution permutation network with the block size of 128 bits and the key size of 128,192 and 256 bits. For security, until now, there is no known practical attack to AES to get the plaintext from the ciphertext. We will use AES for encryption of questions and answers.

B. Asymmetric Key Encryption: RSA

Asymmetric key encryption is a cryptographic protocol which uses different key pairs (private and public) in encryption and decryption. RSA is one of the most preferred asymmetric key encryption method introduced by Ron Rivest, Adi Shamir and Leonard Adleman in 1977 [10]. The RSA public key cryptosystem based on the integer factorization problem. We will use 2048-bit RSA keys in our model. Since the security of RSA is based on the integer factorization problem, there is no active attack to 2048-bit RSA keys.

C. Threshold Cryptography

Threshold cryptography is the distribution of a secret to a group in a multi-sender, multi-receiver systems. In cryptography, the first definition of threshold cryptography was given by Adi Shamir in 1979 [3]. The basic idea of threshold cryptography is sharing a secret. The secret is divided into pieces by the dealer and every piece of it sent to participants. A number of participants should come together in order to get the secret. This is the main idea of $(t, n) - threshold\ cryptosystems$. In $(t, n)-$threshold cryptosystems at least t participants are required for decrypting the secret. In our model, we will use $(t, n)-$threshold cryptosystem where the authority acts as *dealer* and databases are *participants*.

1) Shamir's Secret Sharing: The secret sharing of our model based on *Shamir's Secret Sharing* scheme [3]. Shamir's secret sharing scheme based on polynomial interpolation. Let $s \in \mathbb{Z}_q$ be the secret to be shared where q is prime, t be the number of threshold for reconstructing the secret. The dealer chooses a polynomial $p(x)$ of degree t over $\mathbb{Z}_q$ such that $p(0) = s$. Each participant's secret piece s_i is computed by $p(i)$. Those $p(i)$'s are transmitted into each participant P_i in a secure channel. For reconstructing the secret, at least t participants provide their shares to get s by using polynomial interpolation.

2) Feldman's Verifiable Secret Sharing: If there is a malicious participant in secret sharing scheme, he can deal inconsistent share and reconstructing the secret will be failed. Verifiable secret sharing provides us to compute a procedure where consistent dealings can be verified. Verifiable secret sharing was firstly introduced by Chor et.al., in 1985 [4]. The most common use of verifiable secret share was introduced by Feldman [8]. Feldman's verifiable secret sharing based on Shamir's secret sharing scheme combined with homomorphic encryption scheme. They used the similar idea, trapdoor function, given in RSA. Feldman's verifiable secret sharing scheme works as follows: Let p and q be prime numbers such that $q \mid p-1$. Let $g \in \mathbb{Z}_p$ of order q. The polynomial $p(x)$ over $\mathbb{Z}_p$ with coefficients $p_0, p_1, ..., p_k$ be chosen by the dealer. Then the dealer broadcasts the values $g^{p_0}, g^{p_1}, ..., g^{p_k}$ and secretly transmits the value $s_i = p(i)$ *(mod q)* to each participants P_i. The participants verify their own share by the following equation $g^{s_i} \stackrel{?}{=} (g^{p_0})(g^{p_1})^i(g^{p_2})^{i^2}...(g^{p_k})^{i^k}$ *(mod p)* where one can also consider this $i - adic$ representation of secret. If each participant's share is proper than the equation holds. For completing the dealing of the secret, all participants' share must be proper. We will use Feldman's verifiable secret sharing in our model. The authority will act as dealer and the database servers will act as participants.

III. DATA STORAGE MODEL

In this section, we will propose a new model to store exam materials in a secure way. To achieve the security requirements, we prefer to use verifiable secret sharing scheme to assure long term confidentiality on sensitive data. Our model has four parts: question preparation, question confirmation, storage to database, retrieving data from database. Great amount of data is used in electronic examination. Basically

this data can be personal information of users or questions and answers to be used in exam. The secure storage of this sensitive data is one of the biggest challenge for security. The following questions should be considered for a secure data storage of an electronic exam:

- How the data will be kept in the database such that no one will be able get them without secret key?
- What will happen if the secure algorithm is broken down with today's technology?
- How the integrity of the data is provided?

The answers of above questions can be the change of algorithm when it is broken down. This should be efficient solution to such problems; however, it is not enough if an adversary had retrieved encrypted data before the algorithm was broken down. The other challenge is the integrity of the sensitive data which can be provided by a verifiable mechanism. Therefore, a long term confidentiality with verification of such kind of sensitive data should be provided.

Mainly, the sensitive data for electronic exam is questions and answers. At the first sight, one can define the sensitive data for electronic exam as questions. However, the answers are sensitive data like questions since any adversary can guess the question from the answers with reverse engineering techniques or there is no need to try to solve the questions. So that, both questions and answers should be thought together as sensitive data for electronic exam. These questions and their answers are prepared by question makers for exam and both of them are sent to exam authority. In our model we assume that the channel between authority and question makers is secure. First, we give some notations:

- (P_{QMk}, S_{QMk}), (P_{Aut}, S_{Aut}) are public and private keys for question makers (QMk) and the authority (Aut) relatively,
- $\mathcal{E}$: Encryption function, $\overline{\mathcal{D}}$: Decryption function,
- The package $\mathcal{P} = \{\mathcal{E}_{P_{Aut}}(Q), \sigma_Q\}_{S_{QMk}}$ is a question package where $\mathcal{E}_{P_{Aut}}(Q)$ is the encrypted form of question. The encryption is done by public key of authority and σ is the signature of question signed by question maker.

A. Question Preparation

The security of an electronic exam relies on the security of the questions and answers which are prepared by the question makers. After preparation, they sign their questions, encrypt them with authority's public key and send to authority. Question makers decide the blocks of the question consisting of question part, choices, right answer and tags. The tags consist of question subject, category, subcategory and hardness. The sensitive part of the question blocks are question part, choices and right answer. The other part does not need to be encrypted, because they will be reference for the encrypted questions. A question maker prepares his question and sends to system given in (Fig. 1).

1) Question $Q = \{$*question part, choices, right answer, tags*$\}$
2) Encryption with authority's public key: $\mathcal{E}_{P_{Aut}}(Q)$
3) Signature of question:σ_Q
4) Package to be sent $\mathcal{P} = \{\mathcal{E}_{P_{Aut}}(Q), \sigma_Q\}_{S_{QMk}}$

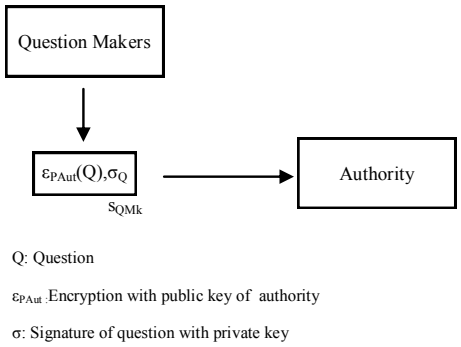

Fig. 1. Question Preparation

B. Question Confirmation

The authority should confirm the valid questions from valid users. The validation is done by the verification of the signature. If the signature is verified, the authority decrypts the question with his private key and edits the question if needed. The edition of the question is done by the editors supplied by the authority. Here, they control the blocks of the questions, revise them if needed and an automatic ID is given. The edited question is separated into two parts: Main and reference.

TABLE I
MAIN PART OF QUESTION

ID	Question Part	Choices	Right Answer
1	.....	.....	.....

TABLE II
REFERENCE PART OF QUESTION

ID	Subject	Category	Subcategory	Hardness
1	.....	.....	.....	.....

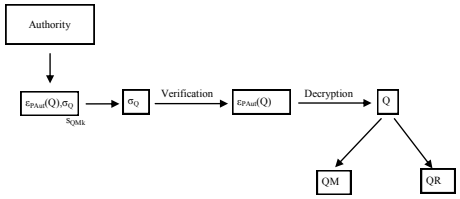

Fig. 2. Question Confirmation

The main part of the question consists of question part, choices and right answer in Table I. The reference part of the question consists of subject, category, subcategory, hardness level in Table II.

1) The authority Aut decrypts the encrypted question $\mathcal{E}_{P_{Aut}}(Q)$ with his private key.
2) Aut verifies the signature of the question σ_Q.

3) After the verification, the question Q is divided into main part QM and reference part QR shown in (Fig. 2).

C. Storage

The storage of the questions is done in two parts: main part of question and reference part of the question. The reference part of the question is not needed to be encrypted since you cannot get the question from the tags of it. They are just kept in the main database of authority.

In our model, the storage protocol consists of n databases where located in different places. The authority acts as *dealer* and sends the questions to other databases. The reference part of questions is stored in the dealer's main database without any encryption. In the storage part we prefer to use AES [7] for

Fig. 3. Storage To Database

symmetric key encryption and verifiable secret sharing scheme [8] for secret sharing. One can also use other cryptographic protocols to provide confidentiality. The storage of the main part of the questions (Fig. 3) is done as follows:

1) The authority i.e., the dealer encrypts the main part of the question with symmetric key encryption: $QM \rightarrow \mathcal{E}(QM)$.
2) Encrypted question $\mathcal{E}(QM)$ is the secret. This secret will be shared with other databases by verifiable secret sharing scheme: $\mathcal{E}(QM) \rightarrow \mathcal{E}(QM)_1, \mathcal{E}(QM)_2, ..., \mathcal{E}(QM)_n$.
3) Every piece of the secret will be transferred into related databases: $DB_1, DB_2, ..., DBn$.

In the storage protocol we use Feldmans's verifiable secret sharing scheme [8] which provides protection of inconsistent dealings of misbehaving dealers. For long term confidentiality, the authority should renew shares periodically. In [9], Ostrovksy and Yung proposed $randomized\ secret$ verified by all dealers and updated by a polynomial. This can be used for renewal process but for consistent sharing and correct dealing of the secret we use Feldmans's verifiable secret sharing. Herzberg et.al., [1] used Feldmans's verifiable secret sharing for share renewal process to get consistent shares and correct dealing of the secret. In our model, we use the same methodology in [1] for periodically update of the share i.e., encrypted form of question pieces for long term confidentiality. Now we will show how verification of and renewal of the share are done?

1) Verification Of The Secret Share: Here we will show that how an encrypted question will be shared into the databases by Feldman's verifiable secret sharing scheme. Let p be a prime, q be a prime such that $q \mid p-1$. Let $g \in \mathbb{Z}_p$ of order q. Then the authority;

1) chooses a polynomial $p(x)$ over $\mathbb{Z}_p$ with coefficients $p_0, p_1, ..., p_k$ explained in Section II,
2) determines the secret is the encrypted form of the main part of question i.e., $\mathcal{E}(QM)$. (Here we assume that $\mathcal{E}(QM) \in \mathbb{Z}_p$),
3) broadcasts the values $g^{p_0}, g^{p_1}, ..., g^{p_k}$,
4) transmits the value of $\mathcal{E}(QM)_i = p(i)$ *(mod q)* to each database servers DB_i

After that process each DB_i should check the equation

$$g^{s_i} \stackrel{?}{=} (g^{p_0})(g^{p_1})^i(g^{p_2})^{i^2}...(g^{p_k})^{i^k} \text{ (mod p).}$$

The equation holds if and only if the share of DB_i is proper. The secret sharing will complete when all DB_i's complete the verification of the equation. The scheme explained above can be done with quantum resistant schemes which is a future work in our proposed model.

2) Renewal Of The Secret Share: For long term confidentiality of any data, the encryption scheme should be updated in some periods. The major concern of this phase is what will happen if an adversary provides inconsistent share updates during the share renewal phase. To solve such scenarios [1] and [5] proposed to use verifiable secret sharing schemes. In our model, we use the same method used in [1]. We perform our share renewal with verifiable secret sharing in order to detect the wrong dealt shares by the database servers. The renewal of the share is done in database servers P_i's as follows:

1) Each P_i defines a polynomial $\delta_i(z) = \delta_{i1}z^1 + \delta_{i2}z^2 + ... + \delta_{ik}z^k$ such that k is random numbers $\{\delta_{im}\}_m$ from $\mathbb{Z}_q$ where $m \in \{1, ..., k\}$.
2) P_i computes $\epsilon_{im} = g^{\delta_{im}}$ *(mod p)* where $m \in \{1, ..., k\}$.
3) P_i computes $u_{ij} = \delta_i(j)$ *(mod q)* where $j \in \{1, ..., n\}$ and $e_{ij} = \mathcal{E}_j(u_{ij}), \forall i \neq j$
4) The message $M_i^{(t)} = (i, t, \epsilon_{im}, e_{ij})$ where $j \in \{1, ..., k\} - \{i\}$ and the signature $\sigma_i(M_i^{(t)})$ is prepared and broadcasted by P_i.
5) P_i decrypts the e_{ij} comes from the other participants, verifies the correctness of the share by the equation explained in Feldmans's Verifiable Secret Sharing Scheme by using $g^{u_{ji}} \stackrel{?}{=} (\epsilon_{j1})^i(\epsilon_{j2})^{i^2}...(\epsilon_{jk})^{i^k}$ *(mod p)*
6) If the messages from other participants are correct, then the above equation holds. Therefore P_i has done the verification and accepted the messages from other participants.
7) P_i updates his own share by $s_i^{(t)} \leftarrow s_i^{(t-1)} + (u_{1i} + u_{2i} + ... + u_{ni})$ *(mod q)* and erases the other variables.

In the above process, if there exists irregularities in the verification part, the dealer must detect the misbehaving participant. Each database server checks the other servers' messages. The participant contacts with the dealer to resolve the inconsistent behaviour when the verification is not done. For this kind of accusation, all honest participants agree on the malicious participant. Then the dealer sends random value to malicious server and wants to encrypt and sign it. If the malicious server (P_d) is not verified by the dealer, then the renewal process updated by the equation:
$s_i^{(t)} \leftarrow s_i^{(t-1)} + \sum_j u_{ji}$ where $j \neq d$ *(mod q)*

D. Retrieving Data

The sensitive data in e-exam, the questions and answers are needed for the exam. The authority should decide which questions are needed for the exam. We separate all questions into two parts: main and reference. The main part of all questions is kept encrypted in the databases. Unlike the main part, reference parts are kept in the main database without any encryption. For preparation of an exam, a committee decides the tags of the questions, i.e., subjects, categories, subcategories and hardness of all questions. With these requirements, the authority selects the questions from reference tables. After that selection, the IDs of questions are determined. For examination, the authority should retrieve the questions with determined IDs. The authority selects the required questions as follows:

1) Let $EXAM = \{ID_1, ID_2, ..., ID_n\}$ be the set of questions to be used in the exam.
2) Let $QUES = \{\mathcal{E}(QM_1), \mathcal{E}(QM_2), ..., \mathcal{E}(QM_n)\}$ be the set of questions to retrieved. Authority assigns each ID in $EXAM$ to $QUES$ respectively.
3) Let $\mathcal{E}(QM_i) = s_r = p^t(r)$ be the secret to retrieved where $r \in \mathcal{B}$ such that $\mathcal{B}$ is the set of servers have incorrect shares.
4) Every database servers $P_i \in \mathcal{D} = \mathcal{A} - \mathcal{B}$ choose k-degree random polynomial δ_i over $\mathbb{Z}_q$ where $\delta_i(r) = 0$ and compute $\delta_{i0} = -\sum_j \delta_{ij} r^j$ *(mod q)*, $j \in \{1, ..., k\}$ where $\mathcal{A}$ is the set of servers.
5) Each P_i broadcasts $\mathcal{E}_j(\delta_i(j))$, $i, j \in \mathcal{D}$.
6) Each P_i's creates new share $s'_r = s_r + \sum_j \delta_j(i)$ and sends to P_r with $\mathcal{E}_r(s'_i)$
7) P_r decrypts the share, and with polynomial interpolation recover s_r
8) The authority uses the key for AES and decrypt $s_r = \mathcal{E}(QM)$ and gets $\overline{\mathcal{D}}(\mathcal{E}(QM)) = QM$ for examination.

IV. Security Analysis

In this section we will give some basic security analysis in order to show that our proposed model is secure. The model based on (t, n)-threshold scheme with verifiable secret sharing scheme assuming that $t - 1 < n/2$.

Theorem 1: If there are at most $t - 1$ malicious database servers, then the proposed protocol reconstruct the secret by honest servers and the system remains secure.

Proof: We assumed that $t - 1 < n/2$ in $(t, n)-$threshold scheme. So that if there are $t - 1$ malicious servers than $t = n/2$ trusted servers. Therefore, the secret is reconstructed by $t = n/2$ trusted server by the definition of secret sharing scheme. ∎

Theorem 2: The proposed data storage protocol possesses authenticity of the servers during the renewal of the secret.

Proof: In the renewal of secret phase, each server P_is should sign a message $\mathcal{M}$ with his private key. The signature of the message $\mathcal{M}$ is verified by each server and Feldman's verifiable secret sharing equation holds. This verification provides authenticity of the servers. ∎

V. Conclusion and Future Works

The development in technology affects almost every area of our life. Especially, the development in digital technology reveals the confidentiality of sensitive data. Electronic learning is today's one of the most popular subject. Nevertheless, electronic exam is also popular cryptographic subject of this branch. In this paper, we propose a new data storage model for electronic exam. We show that the proposed model is secure under the condition of the periodic renewal of the share with the authenticated servers. The model is based on verifiable secret sharing scheme and long term confidentiality. The secrecy of electronic exam is provided by the secrecy of sensitive data which is questions and answers. With the given model, every question encrypt with symmetric key encryption algorithm and split into pieces with verifiable secret sharing scheme. Every piece of encrypted questions are kept in different databases located in different places. The authority is responsible every part of electronic exam, so that for long term confidentiality, the secret shares should be updated periodically by him. As a future work, the given model should be extended to other applications using great amount of data with many users. Also, quantum resistant schemes can be used for the proposed scheme.

Acknowledgment

The authors would like to thank Ali Doğanaksoy for his valuable contributions and feedback.

References

[1] A. Herzberg, S. Jarecki, H. Krawczyk and M. Yung, *Proactive Secret Sharing Or: How to Cope With Prepetual Leakage*, Lecture Notes in Computer Science, Springer-Verlag, 1995, pp:339-352.
[2] A. Huszti and A. Pethö, *A Secure Electronic Exam System*, Publ. Math. Debrecen, 77/3-4, 2010, pp:299-312.
[3] A. Shamir, *How to Share a Secret*, Communications of ACM, 1979, pp:612-613.
[4] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, *Verifiable Secret Sharing and Achieving Simultaneous Broadcast*, Proc. of IEEE, 1985, pp:335-344.
[5] J. Braun, J. Buchmann, C. Mullan and A. Wiesmaier, *Long Term Confidentiality: a Survey*, Designs, Codes and Cryptograpyh, Springer, 2012.
[6] J. Castella-Roca, J. Herrera-Joancomarti and A. Dorca-Josa, *A Secure E-Exam Management System*, Proceeding of the First International Conference on Avaliability, Reliability an Security (ARES'06), 2006, pp:864-871.
[7] J. Daemen and V. Rijmen, *The Design of Rijndale: AES - The Advanced Encryption Standard*, Springer Verlag, Berlin, Heidelberg, New York, 2002.
[8] P. Feldman, *A Practical Scheme for Non-Interactive Verifiable Secret Sharing*, Proc. of the 28th IEEE Symposium on the Foundations of Computer Science, 1987, pp:427-437.
[9] R. Ostrovsky and M. Yung, *How To Withstand Mobile Virus Attacks*, Proc. 10th ACM Conf. on Principle of Distributed Systems, 1991
[10] R. Rivest, A. Shamir and L. Adleman, *A Method For Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, 1978, pp:120-126.
[11] *About The TOEFL PBT Test*, ETS, https://www.ets.org/toefl/pbt/about, 2015.
[12] *How ETS Protects The Integrity of The TOEFL Test*, ETS, https://www.ets.org/toefl/institutions/about/security, 2015.