A Practical E-Test System

https://doi.org/10.3991/ijet.v14i21.10866

Zinah S. Jabbar
University of Imam Ja'afar Al-Sadiq, Baghdad, Iraq
sattarzeina@gmail.com

Abstract—This article presents an encryption system which has many characteristics, like anonymity, originality, correctness, confidentiality, durability and confirmation as well as no need to any trusted authority. Besides that the submitted system gives an evidence of the successful submission by using anonymity property. Additional to use the anonymous return channel, also use the timed-based solution. The proposed system has been implemented and its results were measured. The preliminary findings in this paper seem very promising. Also, the results show that the system is applicable and will yield good results if applied to new generations of mobile phones. Furthermore, the results show that the method is more efficient and faster than the system already in place.

Keywords—E-learning, e-exam system, encryption system, Paillier cryptography system

1 Introduction

In this time, teaching via the programmed systems have fall a new subject because the e-test is the tricky topic in e-learning systems. The e-test operation is the construction of collections for e-learning milieu. Wherein, the e-exam scheme creates safer questions compare to other areas in the e-learning system. Though the e-test system must accomplish the attributes which standard paper-typed tests give, it needs such an e-solution to reduce the work, the time and the cost [1, 2, 3]. The system requirements must totally be satisfied, therefore its plan must consider the extraordinary care for protection. The personally test not just give the ability to ensure student ^{id} , but to check that the students must follow regulations for example students should not speak about any issue related to exam.

There are some problems facing the scheme. First, to recognize the examinees, check them away from the exam-takers, who actually participated in an exam. Alongside, the proposed scheme employs the authentication protocol because it guarantees that cannot manipulate, where a holder of a secret key cannot award the key to others. This technique will allow to the new scheme to discover the fraud, since a private key is utilized in one test only and then will destroy by itself.

A second problem is to control an exam-takers by ensure that they cannot utilized illegitimate stuff. In the proposed e-testing scheme, there is a presence of the exam

office monitored via the director, wherein the test steps are done there by e-means. The scheme is constructed to both written test as well as exam of multiple-choice. So, taken test is passed to educator for marking. The proposed system provides the pseudonym for student as well for the instructor. The educator cannot recognize id for a student in order to avoid his bias also student cannot identify who could correct the test; subsequently he cannot buy the educator for given more scores. The need for pseudonym to student is various from the need for pseudonym to educator. After completing a test, the student will receive the result and then will be concerned on restoring his original id. But, to educator this is not needful, his genuine id must continue confidential.

In 2006, Jordi Castella-Roca et al. [4] proposed an e-test scheme, includes three main participants, the exam manager, teacher and student. The exam manager be in charge of an entire operations including administers questions, solutions and announce the scores. The exam manager is supposed to be impartial; subsequently a system relies on the trusted authority. The exam manager should check the authenticity of the students as well as the teacher using their public and private keys, therefore their genuine id is exposed. However, the objective of the proposed system is to fulfill the pseudonym without need to the impartial exam manager.

However, many e-exam systems are available these days in the markets, but without illustration its security ranks and without mentioned anything about its application problems [5].

2 The E-exam Systems

- It is important to say, the properties of the proposed system are achieved by utilizing the public key encryption systems, so as to specify the student's alias. The student must have its private key when start her studies. Then, a fresh alias will be created to every test derived of the main private key, and have to remain confidential. However, once a test terminate, marks must entered online on the marks file. Thence, it must be capable for recovering a student's public id. It is controlled by timing-expiration, this indicates that prior to an appointed time any person cannot associate the alias with student. However, next a deadline expires; the student id data which provides the relationship among alias combined with contrast student is disclosed. The test manager is not supposed to be honest. Likewise, over an examination operation, both educator and test exam manager have no knowledge about the student's true id. Both of whom they do not have any knowledge whose rectifying an exam sheet for a student. This means that the proposed system ensures that non-disclosure of the identity of educators and students.
- In addition, the proposed system has the whole needful features, and without the use of the trusted authority. Except the registrar which is supposed to be an impartial, where accountable for creating the public and private keys over a preparation phase. Thus, for accomplishing anonymity, n servers are available which offer the timed-based solution. Those servers are making-up the mixed network also, and

because of full talks among participants, must activate and use the anonymous return channel service [6].

2.1 The Security Features

The proposed system features are as follows:

Anonymity: Student might attempt for menacing or buy the educator for obtaining higher score. So, the proposed exam system offers pseudonym to both students besides educators, in order to, the educator has no knowledge of any exam paper for any student when rectifying it, and also the students have no idea whom is rectifying their exam papers. The educators and students will document in absence of disclosing their true ids .

Originality: has to take into account just eligible students exams. It means that, a director should check if an applicant is permitted in participate in the test. Following the registration, the student could disclose its alias to other one requesting him for carry out the exam rather than him. The originality revokes such operation. The students should make certain that have taken the correct questions that are, created via their academy educators. The degree of a test must be checked through the educator, which is selected, that is merely competent educator is permitted for correcting the exam papers.

Correctness: The student is impermissible for performing very similar test more than one time. Also, the formerly submitted test could not be repudiated.

Confidentiality: The testing questions with its solutions must be kept confidential. Throughout a testing procedure must both questions and its created solutions are not allowed detected. Finally, a result of a test must be announced by a way that is simply known to the holder of the corresponding exam.

Durability: The proposed system does not allow to anyone to make any changes to the test questions and solutions once submitted.

Confirmation: once the students have submitted their answers, they must receive a clear confirmation from the exam system about the successful submission.

2.2 The Elements

The participants of the proposed system are as follows:

The Registrar R : generates the exponent and private keys to system participants, as well as creates other keys that require establishing through a setting phase. He is an honest person in the sense that is not conspiring in conjunction with other participants against the system.

The Student S : he wants to pass the test and presumably may be dishonest.

The Educator E : his duties verify the exams, with grant the marks.

The Test Manger M **:** he will issue aliases to qualified participants, administer and validate a testing process, and select educator to an anonymous student. After a test finish, a database will be modernized by student marks.

2.3 Remark

The authors in the proposed test system have utilized the public key encryption system, in particularly, the Paillier cryptography system, in addition to anonymous return channel [6] and timed-based solution. These parts were described in Section 3. The test begins with the registration process, when students and educators obtain the alias. Such pseudonym should be unique to every participant. But, it is unable to connect with the true participant prior to a marking phase. Every participant can only obtain for one alias. The alias is Built by the way that exam manger can check the identity of the participant, and the eligibility for taking the test or correcting the exam paper. Before sending the questions to the student, or sending the answer sheet to the educator. Then, the exam manger checks whether participant possesses an authorized pseudonym. The qualified students receive the test questions, and then they send appropriate solutions after answering the questions. Exam manger verifies whether the student has taken this exam before, if not, sends the answer sheet to an eligible educator, who corrects it after that the corrector sends back to the exam manager the mark of answer of the student. Finally, the exam manager obtains the student's true identity from the alias and the corresponding mark is included.

The proposed system utilizes the Paillier encryption system [7]. The test begins by the initialization phase, once student as well as educator obtains their anonymity, it is impossible to link with an actual participant prior to a scoring period. Every participant obtains only single anonymity. The anonymity is built in the method where a test manager has to check id for a participant with her legitimacy to participate in a test and also in assessing an exam paper. Prior to passing questions for the student and the solution page for the educator, the test manger checks if he has the official anonymity. The authorized student obtains test questions then post related solutions and a period of time. The exam manager verifies if a student was done an exam previously, otherwise passes a solution paper for the authorized educator, which marks it then passes the score back. Finally an exam manger obtains an actual id for student by anonymity then adds a resultant score.

3 Preliminaries

First, some necessary blocks must be built in the proposed system. These are as follows:

3.1 Paillier System

The Paillier system is an asymmetric algorithm. This algorithm can be described as follows:

Algorithm for key generation

- Selects two prime numbers p, q be equally likely [8];
- Computes the $\gcd(pq, (p-1, q-1)) = 1$;

- Finds the modulus $n = pq$;
- Computes $\lambda = lcm(p-1, q-1)$;
- Selects arbitrary number g such that $g \in Z_{n^2}^*$ and ensure that n divides $ord(g)$ via finding a multiplicative inverse ;
- Calculates the inverse $d = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$ such that L be calculated by $L(x) = \frac{x-1}{n}$;
- Determines an encryption key as (n, g) and a secret key is (λ, d) ;

Algorithm for encryption

- Selects the message m such that $0 \le m < n$;
- Chooses arbitrary r where $0 \le r \le n$;
- Encrypts the message m by $c = g^m \cdot r^n \bmod n^2$;

Algorithm for decryption

- To decrypt an encrypted message $m = L(c^{\lambda} \bmod n^2) d \bmod n$;

Remark: Paillier cryptosystem is an asymmetric non-deterministic cryptographic algorithm with homomorphic additive properties. It different from numerous other key-pair systems, Paillier system offers additive homomorphism. It means, the messages could be added to each other during encryption process, and will be decrypt accurately. Paillier manner provides semantic security on a hypothesis that a decisional composite residuosity considered being difficult to solve. Paillier method is a set of hashing of message m and a random integer r . The hash can stop hacker from provide c , and up to alter m . The Paillier algorithm proved secure in the random oracle model. Additive homomorphism is beneficial, because it makes anonymous counting possible. Therefore, it has used in the proposed e-exam system.

3.2 The reusable anonymous return channel

In 2003 Golle-Jakobsson [6] introduced this technique to enable a full anonymous dialogue. This means that, any recipient can transmit anonymous messages, and even transmit one or more anonymous responds to the sender. The performance of such channel is a re-encoding mix-network that uses public-key encryption, relied-on the fact that public-key encryption lets to re-encryption of encrypted messages.

3.3 Time-based solution

The time-based solution is used for obtaining the student identity from a phase for scoring. In registration phase the student is randomly chosen via net, the net have

servers. Assume that $N-t+1$ servers are there. The registrar plays a job of trusted server. The solution steps are as follows:

The server N should do the following:

- Computes message $g_U \bmod n$ as input
- Computes $g_U^{\varpi} \bmod n$ as a result, such that ϖ is a private key, shared between m servers, using (t,m) Shamir secret sharing scheme [9]

The registrar *R* should do the following:

- Selects $m \in Z_n$, represented as x_i with $1 \le i \le m$ for server i and x_i is public
- Selects $a_1, a_2, ..., a_{t-1} \in Z_n$
- Computes $y_i = a(x_i)$, where $1 \le i \le m$
- Passes y_i to server i by the secure manner such that $a(x) \equiv \varpi + \sum_{j=1}^{t-1} a_j x^j \bmod n$
- computes the message using Lagrange interpolation

$g_U^{\varpi} \equiv \prod_{j=1}^{t} g_U^{b_j y_i} \bmod n$, such that $b_j = \prod_{1 \le k \le t, k \ne j} \frac{x_{ik}}{x_{ik} - x_{ij}} \bmod n$;

- Every server saves $(time, y_i, g_U)$
- Issues the time if a server able toward issue the result of g_U
- If time connects t servers compute g_U^{ϖ} as of their shares
- Issues g_U

4 The Proposed E-Exam System

The proposed system was created on some way, so the test manager could run several tests simultaneously. Suppose it is within hand reach many qualified educators for the particular topic. In such a case, the educator can correct more exam papers in more subjects because each educator has qualified certificate. Also, each educator holds digital certificate, and every educator is accountable for its private key, and it is disclosed that the private key has an important benefit to other participants. However, the key generation algorithm relies on mathematical security assumptions.

4.1 Initialization phase

In this phase, the registrar R creates the system keys and the participant keys.
The participant u : should do the following:

- Selects randomly private key $d_U \in Z_n$

- Selects a random number $g_U \in Z_{n^2}^*$
- Computes $e_U \equiv g_U^{d_U} \bmod n$; // the encryption key and private key be used in more than one test

Remark: Assume that a student encryption key (g_S, e_S) , such knowledge concerning who will participate in the test.

The test manager M : should do the following:

- Prior to every test, selects $\bar{s} \in Z_n, \bar{g} \in Z_{n^2}^*$
- declares test keys $(\bar{g}, \bar{h})$ public, such that $\bar{h} \equiv \bar{g}^{\bar{s}} \bmod n$, with $\bar{s}$ private

Remark: Every server obtains couple of keys then together establishes a net.

The trusted committee: should do the following:

- Generates its public key and private key (e_b, d_b)
- Creates the test questions Q
- Posted the questions Q to and ciphered via server encryption key
- Make sure that the validity of these

The text manager M : should do the following:

- Obtains $mix(Q \| \sigma_B(Q \| T_1))$, such that T_1 indicates a time of test begins
- Cannot identify questions Q and is unable to modify such questions Q

However, the proposed system contains three main phases which are as follows:

4.2 Registration phase

The student and the educator anonymity are computed by registrar $(g_U, e_U, d_U, \bar{s}, R)$. The message is posted by the unknown channel. The steps of this phase are as follows:

The exam manger M should do the following:

- A. Ensures that a participant is inside a database
- B. Computes $f = e_U^{\bar{s}} \bmod n$
- C. sends (f, g_U) to server N when the participant U is the student S

The server N should do the following:

- A. Computes $f' = f^{\varpi} \bmod n$
- B. Computes $c = g_U^{\varpi} \bmod n$

- // every server keeps (T, w_i, f, g_U), such that T indicates a time and g_U is public where w_i is the share used by secret sharing
- C. Sends (c, f') to the participant U if U is not

The test manger M should do the following:

- A. Sends (f, g_U) to the participant U

The participant U does the following:

- A. Selects a at random
- B. Computes $f' = f^a \bmod n$
- C. Computes $c = g_U^a \bmod n$
- D. Finds $r = c^{d_C} \bmod n$
- E. Communicates with the exam manger M where M is the prover and user U is the verifier implement the zero knowledge protocol of $(r, f'), (\bar{g}, \bar{h})$; [10]
- F. The participant U should have (c, r, f')

Remark: Assume that authorized student anonymity indicates by (z_1, z_2, z_3) and authorized educator anonymity (y_1, y_2, y_3). The dissimilarity between them merely no wants timed-typed solution to an educator. No want for link its anonymity with its actual id. As indicated previously a student will has his scores once a test terminates, therefore he is keen on improving its actual identity. An educator does not have the same order.

4.3 Testing phase

The test manager M verifies student and educator when both authorized $((z_1, z_2, z_3), subj)$ and $((y_1, y_2, y_3), subj)$ respectively, such that (z_1, z_2, z_3), (y_1, y_2, y_3) are anonymity for student S and educator E. Then, apply algorithm participate in exam $((z_1, z_2, z_3), Q, A, T)$. The steps of this phase are as follows:

The student S should do the following:

- A. Computes the message $m = (z_1 \| z_2 \| z_3 \| subj)$
- B. Sends $C_{mix}(id_S \| e_S)$, $C_{mix}(m)$, $C_{mix}(id_D \| e_D)$ to server, such that id_S is the randomly selected for student S, and e_S is a public key for student S. Participant can utilize diverse id with different public key with every message

The server should do the following:

- A. Gathers the messages with the obvious known time, and every server, then encipher every message again by Paillier system

- B. Sends $C_{mix}(id_S \| e_S)$, $\sigma_{mix}(id_S \| e_S)$, $C_{e_D}(m)$, to the exam manager M such that $\sigma_{mix}(id_S \| e_S)$ is created via server

The educator E should do the following:

- A. Computes the message $((y_1 \| y_2 \| y_3 \| subj)$
- B. passes the message to a test manager by server

The exam manager M should do the following:

- A. Decrypts the message m
- B. Checks a test or scores by
- $z_2^{\bar{s}} \equiv z_3 \bmod n$, or $y_2^{\bar{s}} \equiv y_3 \bmod n$
- C. Verifies if the student S has previously taken the exam
- D. Implements a zero knowledge protocol for identity of a private key of student as well as educator
- E. Enciphers the message by server encryption key;
- F. Saves $((z_1, z_2, z_3), tran_S(y_1, y_2, y_3), tran_I, C_{mix}(id_I \| e_I), subj)$ such that $tran_U$ a copy of $U \in (S, I)$ zero knowledge protocol
- G. Retune the questions by an unknown channel to the student S in the authentic time
- H. Sends $C_{mix}(id_D \| e_D)$, $C_{mix}(m)$, $C_{mix}(id \| e_S)$, $\sigma_{mix}(id_S \| e_S)$ to server with $m = Q_S \| \sigma_B(Q_S) \| T_1$ while $\sigma_B(Q_S)$ indicates a test questions signed via a committee

The student should do the following:

- A. Checks legitimacy of the exam questions
- B. Generates a solution paper A_S
- C. Posts a message $m = z_1 \| y_1 \| C_{mix}(A_S) \| T_2$ by an unknown channel; such that T_2 indicates an actual time of submit test solutions

The test manager M should do the following:

- A. Saves $(Q_S, T_1, T_2, C_{mix}(A_S))$ for each student at his record
- B. Passes a result $H(z_1 \| y_1 \| z_3 \| subj \| tran_S \| Q_S \| T_1 \| T_2 \| C_{mix}(A_S))$ to S as the confirmation
- C. Selects to every submitted test an educator
- D. Sends $C_{mix}(id_{DE} \| e_D)$, $C_{mix}(A_S)$, $C_{mix}(id_I \| e_I))$ to a server, such that id_{DE} is especially created *id* diverse to every test
- E. Securely saves $C_{mix}(id_I \| e_I)$ to a related exam papers

The educator E should do the following:

- A. Marks the test, gives the score
- B. Posts a message by an unknown channel $m = (grade \| H(grade \| A_S) \| [H(grade \| A_S)]^{d_I} \| noinarans)$, such as noinrans is a copy of zero knowledge protocol of integer factoring of $(H(grade \| A_S), [H(grade \| A_S)]^{d_I}, y_1, y_2)$;

The test manager M should do the following:

- A. Once a test ended must hold the students anonymity with related scores

4.4 Marking phase

Following the actual time determined on a threshold for a test timed-typed solution creates basic information to anonymity to recover an actual id of students, test manager and server implement $getid(z_3, T)$ algorithm. The information is post by the unknown channel. The steps of this phase are as follows:

The test manager M should do the following:

- A. Finds $z_1 \equiv g_S^{\Gamma} \bmod n$
- B. Finds $z_2 \equiv e_S^{\Gamma} \bmod n$
- C. Finds $z_3 \equiv e_S^{\Gamma_{\bar{S}}} \bmod n$;
- D. Passes z_3 to server N such that z_3 is a parameter of student (z_1, z_2, z_3) anonymity

The server N should do the following:

- A. Finds $z_3 \equiv z_4^{\varpi} \bmod n$
- B. Passes z_3 to the test manager M

The test manager M should do the following:

- A. Decrypts message
- B. Obtains student actual id using (z_3, z_4)
- C. Adds $C_{mix}(id_I \| e_I)$ and $H(grade \| A_S) \| [H(grade \| A_S)]^{d_I} \| nomtats$, and the scores to a student record

4.5 Security discussion

The proposed test system has the following properties:

Anonymity: The student S and the educator E pseudonym can reach via using aliases with the unknown send back channel. The student alias is created via the test manager M with sever N . The server N computes $g_S \bmod n$ then find

$z_4 \equiv e_S^{\bar{s}} \bmod n$ for students, since the test manger M is unable to link $z_1 \equiv g_S^{\varpi} \bmod n$ with $(z_3 \equiv z_4^{\varpi} \bmod n)$ by (g_S, z_4). The educator E anonymity is computed via an educator E using the Shamir secret sharing algorithm, thus just the allowed group of servers can create a randomized anonymity. Assume that no less than $n-t+1$ servers, since a randomized alias is unable to linked with an actual id. In fact, the actual id for student is not exposed until a phase for scoring. Finally, the student id must be recovered via the timed-type solution.

Originality: throughout a test phase when authorized $((z_1, z_2, z_3) \| subj)$ also when authorized $((y_1, y_2, y_3), subj)$ algorithms ensure the authenticity for students and educators. The test exam manger M makes sure if anonymity is eligible to a related topic, it means that $z_2^{\bar{s}} \equiv z_3 \bmod n$, $y_2^{\bar{s}} \equiv y_3 \bmod n$ such that $\bar{s}$ is a private key for a known topic. If congruence is true, the test manager M checks if sender is a holder for an alias via using the zero knowledge protocol for private key of (z_1, z_2) with students (y_1, y_2) with educators. Any more student, unlike of anonymity holder, will unable to participate in an exam by free of facts about a private exponent. When the student S_1 provides the results of z_1, z_3 for a new student S_2 inquiring S_2 to solve test papers, will be discovered in a zero knowledge protocol, because S_2 is not identified S_1 private exponent and when S_2 uses her private key for obtaining z_2, an alias is not allowed to a related test. A simply manner to obtain the right anonymity when S_1 discloses her private exponent to S_2. Suppose that the students take exam papers at a test phase during step 5, a real time with a board signature, showing the validity of those. Score authentic via a related educator is added to a record by a zero knowledge protocol.

Correctness: In the test phase in step 4, the test manager M verifies if a student S attended the exam previously, if she did, the test manager M will not care about a second exam. If the student S is taken the exam, will be fixed via the educator E then a student id is exposed, she will not able to disavow it.

Confidentiality: verification is showed by the copy from the zero knowledge protocol which is added in a record. The student can check if the solution is not changed via an acknowledgment then details added plus a score to a record. The questions and solutions are transmitted enciphered by an exponent key from server, thus will not recognized via new participant. Finally the student sees just her personal score.

Durability: prior to test begins the test manager M be given an enciphered, authorized questions as of the board $(C_{mix}(Q \| \sigma_B(Q) \| T_1))$, since both the test manager M and participants cannot identify these questions thus unable to alter these. In a test phase, in step 6. The student checks legitimacy of these. The student passes enci-

phered solutions $(C_{mix}(A_S))$ to the test manager M. The test manager M sends them toward the educator E. An educator E as soon as assess these posts $grade \| H(grade \| A_S) \| [(grade \| A_S)]^{d_I} \| noinrans$ to the test manager M, whilst a score with a related solution is mix up then validated via an educator E.

Confirmation: In a test phase in step 7 the test manager M computes and issues the value as follow $H(z_1, z_2, z_3, subj, tran_S, Q_S, T_1, T_2, C_{mix}(A_S))$ as the confirmation of a student.

4.6 Remarks

When the student asks questions concerning her exam following the result, she is able to inquire an educator that scored her exam paper. In addition, her score is given $C_{mix}(id_I \| e_I)$ too. A student sends $C_{mix}(id_S \| e_S)$, $C_{mix}(Q)$, $C_{mix}(id_I \| e_I)$ to a server, a related educator has capability for solving questions namelessly by an unknown return channel. Suppose that there is the determined time to submit questions with solutions, thus there must be satisfactory messages to a server.

5 Conclusion

It can emphasis a high transparent with considerable durability in the system where used, it is a best and efficient e-test scheme is reached. From the practical side, a present authentication technique, facing some considerable restrictions. However, the authentication and the anonymity may be a good transparent. Equally, a durability and correctness study come from a majority of participant activities.

In the future, a study will concentrate on enhancement the system to be quite efficient by applying the transparent, and much adaptable, and also unbroken authentication technique. To check n test of participant, make sure merely an authorized student is attended a test, a system shall provide unbroken participant id using face recognition is one of a clear biometric for keeping track of a student movement.

6 References

[1] Moustafa Al-Fayoumi, Sattar J Aboud, An Efficient E-Exam Scheme, International Journal of Emerging Technologies in e-learning (iJET) - Vol. 12, No. 4, pp. 153-162, 2017. https://doi.org/10.3991/ijet.v12i04.6719

[2] Sattar J. Aboud, Secure E-Exam Scheme, International Journal of Science and Research (IJSR) 3(9), pp. 2200-2203, 2014

[3] Mohammad A. Al-Fayoumi, Sattar J. Aboud, Mamoun S. Al-Rababaa, Secure E-Test Scheme, International Journal of Emerging Technologies in Learning (iJET), Vol. 2, No. 4, 2007.

[4] Castella-Roca, J. Herrera-Joancomarti and A. Dorca-Josa, A secure e-exam management system, Proceeding of the First International Conference on Availability, Reliability and Security (ARES'06), 2006, 864–871. https://doi.org/10.1109/ares.2006.14
[5] Barhoom and Shen-Sheng Zhang, Trusted exam marks system at IUG using XML-signature, Proceeding of the Fourth International Conference on Computer and Information Technology (CIT'04), 2004, 288–294. https://doi.org/10.1109/cit.2004.1357210
[6] Golle and M. Jakobsson, Reusable anonymous return channels, Proceeding of the 2003 ACM workshop on Privacy in the e-society, 2003, 94–100. https://doi.org/10.1145/1005140.1005155
[7] Paillier, Pascal (1999), "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", *EUROCRYPT* Springer, pp. 223–238 https://doi.org/10.1007/3-540-48910-x_16
[8] Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography: Principles and Protocols," Chapman & Hall/CRC, 2007
[9] Shamir, How to share a secret, Comm. ACM 22 (1979), 612–613
[10] Menzenes, van Oorschot, Vanstone, Handbook of Applied Cryptography, 1996.

7 Author

Zinah S. Jabbar is a lecturer in Information Technology College, University of Imam Ja'afar Al-Sadiq, Baghdad-Iraq, sattarzeina@gmail.com

Article submitted 2019-05-15. Resubmitted 2019-06-30. Final acceptance 2019-07-04. Final version published as submitted by the authors.