Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2022) 30: 361 – 375

doi:10.3906/elk-2105-204

Permissioned Blockchain based Remote Electronic Examination

Oznur KALKAR*, **Isa SERTKAYA**
MCS Labs & BCLabs, TÜBİTAK BİLGEM UEKAE, PK. 74, 41470, Gebze, Turkey,

Received: 20.05.2021 • **Accepted/Published Online:** 10.01.2022 • **Final Version:** 04.02.2022

Abstract: Recent coronavirus pandemic transformed almost all aspects of daily life including educational institutions and learning environments. As a result, this transformation brought remote electronic examination (shortly e-exam) concepts back into consideration. In this study, we revisit secure and privacy preserving e-exam protocol proposals and propose an e-exam protocol that utilizes decentralized identity-based verifiable credentials for proof of authentication and public-permissioned blockchain for immutably storing records. In regard to the previously proposed e-exam schemes, our scheme offers both privacy enhancement and better efficiency. More concretely, the proposed solution satisfies test answer authentication, examiner authentication, anonymous marking, anonymous examiner, question secrecy, question privacy, mark privacy, test verifiability, and mark verifiability properties.

Key words: Electronic exams, e-exams, decentralized identity, verifiable credentials, security, privacy, permissioned blockchain

1. Introduction

The coronavirus has spread around the globe, affecting almost all nations and territories. In order to flatten the curve and decrease the spread of the disease, lockdown and stay-at-home methods have been implemented. These lockdown and stay-at-home strategies resulted in the closing of colleges, training institutions, and higher education facilities. However, it also opened a door to mass adoption of remote education. Despite the difficulties faced by both educators and learners, educators are delivering quality education across multiple online channels, which is a paradigm change.

Transitioning into e-learning systems also brought growing demand for tools remotely evaluating skills and knowledge of the trainees. Even though the pandemic certainly increased the demand, secure schemes for online examinations can be very useful even if there is no pandemic. However, making exams online brings new attack surfaces to the exams. Authentication and proctoring can be given as an example. Candidates (or students) may want someone to take the exam for them or may try to cheat during the exam. Also, secrecy of the individual's answers should be satisfied in order to prevent other candidates to copy answers. These security threats must be addressed. There are also problems regarding privacy of the candidates, for instance a candidate's mark should be kept secret from the other candidates.

Generally, traditional exams involve three entities and four phases. Firstly, during the *registration* phase, the *exam authority* organizes the exams and the *candidates* sign up for it. Then, at the *testing* phase, candidates receive the exam and submit their answers. Next, during the *marking* phase, the *examiners* receive and evaluate the candidates' answers. Finally, the exam authority registers the candidates' marks, and the candidates learn

*Correspondence: oznurarabaci@gmail.com

their marks at the *notification* phase.

Multiple-choice, truth or false, matching, arrangement, fill in the blank, essays, and other types of questions are included in an e-exam. There is a distinction to be made between a remote electronic exam (or shortly e-exam) and a computer-based assessment, which relies on the use of specialized software that is not linked to the internet. Network-based assessment, on the other hand, is based on the use of internet techniques such as a remote exam network, [1]. Here, we consider network based assessments.

E-exams are organized following the same principles of traditional exams and require the same main security and privacy features. Naturally, in traditional face-to-face exams, candidate authentication and exam rules compliance can be checked more easily. However, e-exam schemes require specific security and privacy concerns on authentication due to the increased attack surface. Besides authentication, candidates that take the exam should be proctored for cheating.

Although more attention should be given to the misconducts committed by the candidates than the exam authorities, exam authorities may also behave maliciously and cause misconducts that are hard to notice,[2]. One of the largest scandals involving authorities in United States history took place in 2009. The Atlanta Journal-Constitution published analyses of Criterion-Referenced Competency Tests (CRCT) results, which showed statistically unlikely test scores, including extraordinary gains or losses in a single year. An investigation by the Georgia Bureau of Investigation released in July 2011 indicated that more than 150 teachers and administrators from 44 out of 56 public schools across Atlanta were caught changing answers on standardized tests used to judge student performance and rank schools on the 2009 CRCT[1]. On April 1, 2015, eleven of the twelve defendants were convicted of racketeering and sentenced to 5–20 years in prison, [3]. In order to avoid these kind of malicious behaviour of authorities, the e-exam system should be designed carefully. For further details of such scandalous occurrences, please refer to [3] and Washington Post's news about Atlanta public schools[2].

There are various e-exam proposals that aim to assure security and privacy as summarized in the sequel. In this study, we present an e-exam solution based on blockchain and anonymous verifiable credentials and discuss the security and privacy of the proposed scheme.

1.1. Related works

Online exam proposals dates back to 2006. Castella-Roca et al. [4] introduced a secure e-exam management system with trusted exam authority who is fully trusted for assuring candidate's privacy. Later, [5] proposed to reduce [4]'s trust assumptions by utilizing pseudonyms for the candidates. However, Dreier et al. [6] showed that [5]'s scheme suffers from several security flaws. Next, Giustolisi et al. [7] proposed an e-exam protocol called Remark! that utilizes a mix net with at least one honest entity and uses a bulletin board. Bella et al. [2] propose a secure exam protocol that does not rely on any trusted party by relying on oblivious transfer and visual cryptography schemes.

[8] proposed an e-exam system called ExamShield that again fully trusts the exam authorities and focus on biometric authentication that further involves mouse dynamics, keystroke dynamics, and face biometrics.

[1] abcNEWS (2011). Atlanta Cheating: 178 Teachers and Administrators Changed Answers to Increase Test Scores [online]. Website https://abcnews.go.com/US/atlanta-cheating-178-teachers-administrators-changed-answers-increase/story?id=14013113 [accessed January 2021].

[2] Washington Post (2011). Atlanta public schools embroiled in cheating scandal [online]. Website https://www.washingtonpost.com/blogs/blogpost/post/aps-atlanta-public-schools-embroiled-in-cheating-scandal/2011/07/11/gIQAJl9m8H_blog.html [accessed January 2021].

Islam et al. designed a blockchain based exam system named BSSSQS[3]. They address the problem of question leaking, and their solution depends on encryption and randomization of the questions. However, they only deal with the delivery of the questions to the candidates.

Mitchell et al. [9] proposed a decentralized application for an examination review called "dAppER". In fact, dAppER implements existing procedures and documents them on a permissioned blockchain to ensure irreversibility, immutability, and auditability. Deborah et al. [10] focuses on a simple e-exam scheme for mutual authentication between the candidate and the server and secure delivery of question paper from the server. However, both of these proposals unfortunately assume the exam authorities are trusted and will not act maliciously. Therefore, they can not determine the misconducts, summarized in [3] and Washington Post's article[4], caused by the exam authorities.

For a recent survey on online exams, reader may refer to [11]. Of all the examined papers, there are three that focus on security. [12] focus on authentication and authorization of the candidates and aim to protect security and integrity of the questions. [14] propose to use graphical own image password to eliminate the modifications in the result and generation of fake question papers. [13] aims to improve availability of e-exam, which is implemented in wireless network. In case of connection problem, this model automatically provides additional time. None of these papers handles marking and notification. In addition to that, they do not fulfill the e-exam security and privacy requirements that are summarized in Section 2.3.

Even if there exists many computer-based exam management systems, most of these system designs rely on trusted exam authorities, please refer to [1] for a recent e-exam survey. There are only a few proposals that rely solely on cryptographic primitives to assure security and privacy.

1.2. Our contributions

In this manuscript, we give an online exam proposal based on blockchain, which eliminates the need of bulletin boards. As illustrated in Figure 1, Our proposal also uses a blind signature scheme, which helps to achieve anonymity of the users without using mix nets or trusting a third party. Moreover, due to the nature of the blockchain, the data remains indefinitely and unchanged, which also makes audit procedures much easier.

1.3. Organization

Organization of the manuscript is as follows. Preliminaries, security model, and cryptographic building blocks used in the proposed secure e-exam scheme are summarized in Section 2. The new secure and privacy enhancing e-exam protocol is proposed in Section 3. A discussion on security and privacy of the proposed mechanism is given in Section 4, and finally Section 5 concludes the manuscript.

2. Preliminaries

2.1. Electronic exam

As illustrated in Figure 1, typically, there are three types of entities involved in an exam: candidates (c), examiners who grade the exams (e), and an exam authority (EA) that takes part in the organization and execution of the exam. E-exams and traditional exams consist four phases: registration, testing, marking, and

[3]A. Islam, Md. F. Kader, and S. Y. Shin (2018). BSSSQS: A Blockchain Based Smart and Secured Scheme for Question Sharing in the Smart Education System [online]. Website https://arxiv.org/abs/1812.03917 [accessed January 2021].

[4]Washington Post (2011). Atlanta public schools embroiled in cheating scandal [online]. Website https://www.washingtonpost.com/blogs/blogpost/post/aps-atlanta-public-schools-embroiled-in-cheating-scandal/2011/07/11/gIQAJl9m8H_blog.html [accessed January 2021].

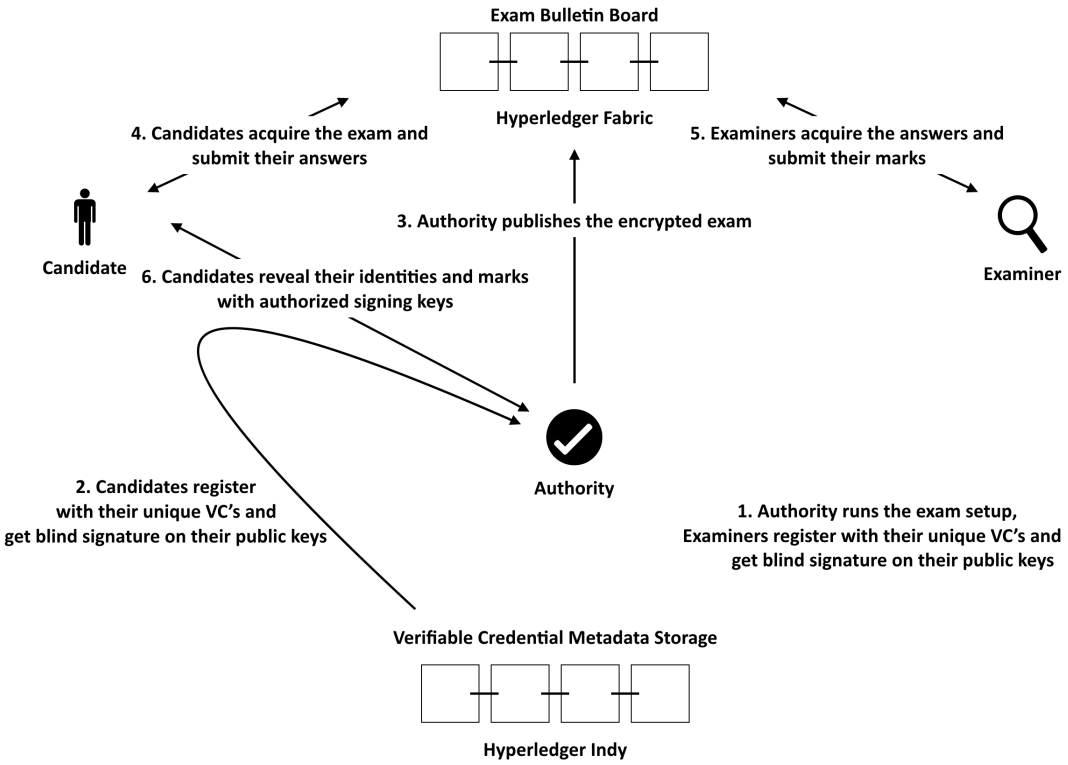

Figure 1. Architectural overview of the proposed secure e-exam scheme.

notification. The exam authority arranges the exam and candidates enroll for the exam during the registration phase. Testing phase is the phase where candidates receive and take the exam and submit their answers. Examiners receive and grade the answers during marking phase. Finally, candidates learn their marks in the notification phase.

2.2. E-exam threats

In our scheme, we aim to rule out the following threats same as Remark! scheme proposed in [7].

1. An intruder impersonating a candidate during the testing.
2. An intruder tampering with a candidate's test answer or mark.
3. A candidate seeking to get higher mark than she deserved.
4. A candidate seeking to coerce the examiner who evaluates her test.
5. The manager tampering with the marks.
6. An examiner seeking to assign a biased mark to a specific candidate's test.

2.3. E-exam security and privacy requirements

In this subsection, we give the security requirements that a secure e-exam should satisfy. These requirements follow from the previous studies [15] and [7].

- Test Answer Authentication. The exam authority only accepts test answers submitted by registered candidates.
- Examiner Authentication. The exam authority only accepts evaluations provided by a registered examiner.
- Anonymous Marking. No one learns the author of a test answer before the test is marked.
- Anonymous Examiner. No candidate learns the identity of the examiner who evaluates their test answers.
- Question Secrecy. No candidate learns the test question before the testing phase begins.
- Question Privacy. The exam authority does not learn which test question is assigned to a specific candidate.
- Mark Privacy. The candidate learns only her mark and not those of other candidates.
- Test Verifiability. The candidate can verify that her test is considered for evaluation.
- Mark Verifiability. The candidate can verify that the exam authority registers the mark she was assigned to by the examiner, and the exam authority can verify that the candidate gets the mark she was given by the examiner.

2.4. E-exam assumptions

Design and analysis of the proposed online exam scheme rely on the following assumptions:

1. We assume that there exists an authentication mechanism for the exam authority to authenticate the candidates and the examiners at the beginning of the registration phase. This can be realized for example anonymous credential [16] based self-sovereign identity solutions [5].
2. To mitigate cheating, candidates are invigilated during the testing phase.
3. A private, permissioned blockchain is already established and ready to use.

2.5. Notations

In the sequel, κ is the security parameter and "$\leftarrow$" and "$\leftarrow_{\$}$" denote assigning an output value to a specific variable and to a uniformly distributed variable of a set, respectively. $\{0,1\}^*$ and $\{0,1\}^\kappa$ respectively denote an arbitrary length bit-string and a bit string of length κ.

The notation $[a]P$ corresponds to a scalar multiplication, in an additive group, of a generator $P \in \mathbb{G}$ of order p by a scalar $a \in \mathbb{Z}_p$, i.e., $P + P + \cdots + P$, a times. We will use the following primitives

- Online exam $\mathsf{Exam} = \{\mathsf{Setup}, \mathsf{Registration}, \mathsf{Testing}, \mathsf{Marking}, \mathsf{Notification}\}$, each phase is defined as follows:
  - Setup: Secret keys of the EA and public parameters of the scheme is output as $\mathsf{pp}_{\mathsf{ex}}$.
  - $\mathsf{Registration}$: Candidates and examiners follow the registration phase together with the exam authority in order to register their pseudonyms.
  - $\mathsf{Testing}$: Exam authority and the candidates perform this phase. EA publish the test questions for the candidates, candidates solve the questions, append their answers to the questions, and publish.

[5] Sovrin Foundation (2016). Sovrin: Digital Identities In The Blockchain Era [online]. Website https://sovrin.org/library/sovrin-digital-identities-in-the-blockchain-era/ [accessed January 2021].

- Marking: Examiners get the answers and questions of the candidates, mark them, and publish the marked answers.
- Notification: During this phase, candidates' marks are registered by EA.

- Cryptographically secure hash-function $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^\kappa$,
- Digital signature scheme $\mathsf{Sig} = (\mathsf{G_{sig}}, \mathsf{K_{sig}}, \mathsf{S_{sig}}, \mathsf{V_{sig}})$ where
  - Setup $(\mathsf{pp_{sig}} \leftarrow \mathsf{G_{sig}}(\kappa))$: Given a security parameter κ, yields public parameters as $\mathsf{pp_{sig}}$,
  - Keygen $((\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{K_{sig}}(\mathsf{pp_{sig}}))$: Given public parameters $\mathsf{pp_{sig}}$, generates a private and public signing key pair,
  - Sign $(\sigma \leftarrow \mathsf{S_{sig}}(\mathsf{sk}, m))$: Given private signing key sk and a message m, signature σ for the message m is generated,
  - Verify $(\{0,1\} \leftarrow \mathsf{V_{sig}}(\mathsf{pk}, m, \sigma))$: Given public key pk, a message m and signature σ, outputs 1 if the signature σ is valid, otherwise outputs 0.
- Public key encryption scheme $\mathsf{Pec} = (\mathsf{G_{pec}}, \mathsf{K_{pec}}, \mathsf{E_{pec}}, \mathsf{D_{pec}})$ where
  - Setup $(\mathsf{pp_{pec}} \leftarrow \mathsf{G_{pec}}(\kappa))$: Given a security parameter κ, outputs public parameters as $\mathsf{pp_{pec}}$,
  - Keygen $((\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{K_{pec}}(\mathsf{pp_{pec}}))$: Given public parameters $\mathsf{pp_{pec}}$, generates a private and public encryption key pair,
  - $\mathsf{Encrypt}$ $(c \leftarrow \mathsf{E_{pec}}(\mathsf{pk}, m))$: Given public key pk and a message m, encrypts the message m and outputs ciphertext c,
  - $\mathsf{Decrypt}$ $(m \leftarrow \mathsf{D_{pec}}(\mathsf{sk}, c))$: Given private key sk and a ciphertext c, decrypts c to m.

2.6. Verifiable credentials

Decentralized identity (or Self-sovereign identity (SSI)) aims to give identity owners complete control over their identities, as well as protection, privacy, and a single management process for both physical and digital identities. To build permanent identity records, SSI solutions combine distributed ledger technology with verifiable credentials. SSI, unlike previous identity management solutions, allows the verifier to verify who provided the credential, if it was issued to the presenter, if it has been tampered with, and if it has been withdrawn without having to contact the issuer. In this regard, as illustrated in Figure 2, a verifiable credential is a set of tamper-evident claims and metadata that cryptographically prove who issued it. Users are holders that receive issued credentials. Issuers grant and verify the credentials of the users. Verifiers verify credentials of the users presented in plain, partially or fully hidden form.

Our scheme assumes existence of an SSI mechanism, and each entity holds a set of verifiable credentials to prove her identity and use for authentication. For concrete SSI primitives, please refer to [16] and Sovrin's self-sovereign identity[6].

[6]Sovrin Foundation (2016). Sovrin: Digital Identities In The Blockchain Era [online]. Website https://sovrin.org/library/sovrin-digital-identities-in-the-blockchain-era/ [accessed January 2021].

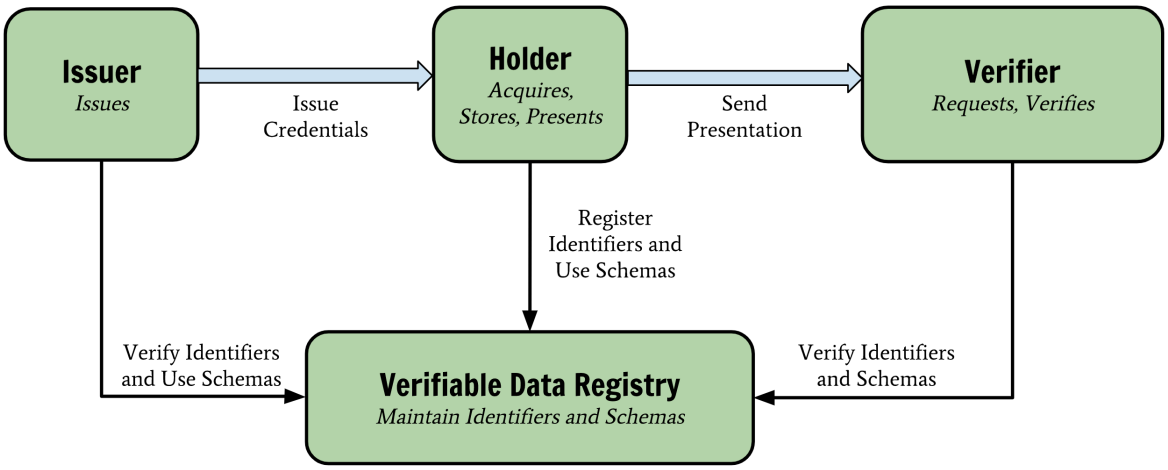

Figure 2. The roles and information flows in W3C verifiable credentials data model.

2.7. Permissioned blockchain

A blockchain is an immutable transaction ledger that is maintained by a distributed network of nodes, with each node maintaining a copy of the ledger by appending new transactions that have been checked by a consensus protocol. The data on the ledger is organized into blocks, each of which has a hash that links it to the one before it. While public permissionless blockchains allow anyone to write on the ledger, permissioned blockchains follow a governance model that allows only approved nodes to write on it.

Although this system can be realized on existing public blockchains, students and examiners would need to pay fees to the miners to get their transactions written to the ledger. In order to avoid changing costs and being dependent on systems' performance to process transactions, we believe it would be better if this system uses its own blockchain. Permissioned blockchain is chosen over permissionless, since it is faster, more scalable, energy-efficient, and participants(schools) are known beforehand.

One example of permissioned blockchain is Hyperledger Fabric that has been developed under the Linux Foundation as an open source project, [17]. Our scheme utilizes a permissioned blockchain as an append-only immutable bulletin board.

3. Proposed protocol

Proposed protocol is illustrated in Figure 1. In a nutshell, the protocol is pursued as follows.

- The exam authority EA determines Pec and Sig primitives, runs Setup phase for generating system-wide public parameters and her key pairs for blind Schnorr signature scheme,
- At the Registration phase, the candidate C proves her identity using her verifiable credentials to EA and requests EA to blindly sign her public keys,
- Following EA's randomly pairing candidates and examiners and generating test questions, C takes the test during the Testing phase. After answering the questions, C signs her answers and encrypts for the examiner.
- During the Marking phase, the examiner decrypts the answers, marks the test, appends her mark, signs and encrypts for the candidate.

- The candidate decrypts the examiner's mark, learns her mark, adds her identifying information to bind the public keys to her real identity, and encrypts for the exam authority. The exam authority decrypts that information matches the public keys of the candidate to the candidate's real identity and saves the candidate's mark at the end of Notification.

For concrete instantiation of the proposed protocol,

- verifiable credentials and corresponding metadata can be stored on Hyperledger Indy[7].
- ElGamal encryption scheme[18] can be utilized for Pec scheme.
- Schnorr signatures[19] can be utilized for Sig scheme.
- Blind Schnorr signature scheme will be used for blindly signing the public keys of the examiners and candidates.
- the permissioned blockchain that will be utilized as bulletin board can be Hyperledger Fabric[8].

There is a famous chart in NIST's technical report (Page 42, Figure 6)[9] that guides someone to decide if they really need a blockchain for their problem. Referring to the mentioned figure, online-exam system needs a shared, consistent data store in order to archive exams, there are more than one entity(schools, students, teachers)that contributes to the data, data records are never updated or deleted, sensitive identifiers are not stored on the blockchain(exams, answers, and marks are encrypted; identities of students and examiners are anonymous), since the exam system is nation-wide or even global, entities can not decide who should be in control of the data store, and finally a tamper-proof log of all writes to the data store are required for any dispute resolution.

In this manuscript, we treat Pec and Sig algorithms as black-box, since any CCA-secure encryption algorithm and existentially-unforgeable signature algorithm can be utilized as Pec and Sig, respectively. However, since the blind signature algorithm is crucial for the protocol, we give it in detail in the Setup and Registration phases even though we just follow blind Schnorr signature scheme. More concretely, steps 6-9 and steps 2-5 of Setup and Registration phases correspond to the blind Schnorr signature scheme.

3.1. Setup

During the Setup phase, the exam authority EA publishes the exam public parameters $\mathsf{pp}_{\mathsf{ex}}$ and examiners register themselves for the exam.

1. EA determines a public key encryption scheme Pec that is going to be used for encrypting and decrypting questions, answers, and marks and generates its public parameters $\mathsf{pp}_{\mathsf{pec}}$.
2. EA determines a digital signature scheme Sig that is going to be used to sign questions, answers, and marks and generates its public parameters $\mathsf{pp}_{\mathsf{sig}}$ along with its signing key pair $(\mathsf{sk}_{\mathsf{sig}}^{\mathsf{EA}}, \mathsf{pk}_{\mathsf{sig}}^{\mathsf{EA}})$.

[7]Hyperledger Foundation. Hyperledger Indy [online]. Website https://hyperledger-indy.readthedocs.io/en/latest/ [accessed January 2021].

[8]Hyperledger Foundation. Hyperledger Fabric [online]. Website https://www.hyperledger.org/use/fabric [accessed January 2021].

[9]NIST (2018). NISTIR 8202 - Blockchain Technology Overview [online]. Website https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf [accessed January 2021].

3. EA generates the public parameters for blind Schnorr signature scheme $\mathsf{pp_{Sch}} = (p, \mathbb{G}, P, \mathcal{H})$ along with its signing key pair $(\mathsf{sk^{EA}_{Sch}}, \mathsf{pk^{EA}_{Sch}})$, where $\mathsf{sk^{EA}_{Sch}} \leftarrow_{\mathsf{r}} \mathbb{Z}_{\mathsf{p}}, \mathsf{pk^{EA}_{Sch}} = \mathsf{xP}$.

4. EA publishes the exam public parameters $\mathsf{pp_{ex}}$ as

$$\mathsf{pp_{ex}} \leftarrow (\mathsf{pp_{pec}}, \mathsf{pp_{sig}}, \mathsf{pp_{Sch}}, \mathsf{pk^{EA}_{sig}}).$$

5. e proves herself to EA using verifiable credentials .

6. EA chooses $r \leftarrow_r \mathbb{Z}_p$, computes $R' \leftarrow [r]P$ and sends R' to e.

7. e creates key pairs for encryption and signature algorithms,

$$(\mathsf{sk^e_{pec}}, \mathsf{pk^e_{pec}}) \leftarrow \mathsf{K_{pec}}(\mathsf{pp_{pec}}),$$
$$(\mathsf{sk^e_{sig}}, \mathsf{pk^e_{sig}}) \leftarrow \mathsf{K_{sig}}(\mathsf{pp_{sig}}),$$

chooses $\alpha, \beta \leftarrow_r \mathbb{Z}_p$, computes

$$R \leftarrow R' + [\alpha]P + [\beta]\mathsf{pk^{EA}_{Sch}}$$
$$c \leftarrow \mathcal{H}(R, \mathsf{pk^e_{pec}}||\mathsf{pk^e_{sig}})$$
$$c' \leftarrow c + \beta \mod p,$$

and sends c' to EA.

8. EA computes $s' \leftarrow r + c'x \mod p$ and sends s' to e.

9. e checks if

$$[s']P = R' + [c']\mathsf{pk^{EA}_{Sch}},$$

computes $s = s' + \alpha \mod p$ and EA's signature on $\mathsf{pk^e_{pec}}||\mathsf{pk^e_{sig}}$ is

$$\sigma_{\mathsf{e}} \leftarrow (R, s).$$

10. e sends $(\mathsf{pk^e_{pec}}||\mathsf{pk^e_{sig}}, \sigma_{\mathsf{e}})$ to the blockchain along with a signature on it signed using $\mathsf{sk^e_{sig}}$.

11. Nodes first verify the outer signature by $\mathsf{pk^e_{sig}}$, then checks if

$$[s]P = R + [c]\mathsf{pk^{EA}_{Sch}},$$

where

$$c = \mathcal{H}(R, \mathsf{pk^e_{pec}}||\mathsf{pk^e_{sig}}).$$

If only all the checks holds, the transaction is added to the ledger.

3.2. Registration

After the examiner registration is completed, an eligible candidate c and the exam authority EA performs the registration phase together.

1. c proves herself to EA using verifiable credentials .

2. EA chooses $r \leftarrow_r \mathbb{Z}_p$, computes $R' \leftarrow [r]P$ and sends R' to c.

3. c creates key pairs for encryption and signature algorithms,

$$(\mathsf{sk}^{\mathsf{c}}_{\mathsf{pec}}, \mathsf{pk}^{\mathsf{c}}_{\mathsf{pec}}) \leftarrow \mathsf{K}_{\mathsf{pec}}(\mathsf{pp}_{\mathsf{pec}}),$$
$$(\mathsf{sk}^{\mathsf{c}}_{\mathsf{sig}}, \mathsf{pk}^{\mathsf{c}}_{\mathsf{sig}}) \leftarrow \mathsf{K}_{\mathsf{sig}}(\mathsf{pp}_{\mathsf{sig}}),$$

   chooses $\alpha, \beta \leftarrow_r \mathbb{Z}_p$, records β, computes

$$R \leftarrow R' + [\alpha]P + [\beta]\mathsf{pk}^{\mathsf{EA}}_{\mathsf{Sch}}$$
$$c \leftarrow \mathcal{H}(R, \mathsf{pk}^{\mathsf{c}}_{\mathsf{pec}} || \mathsf{pk}^{\mathsf{c}}_{\mathsf{sig}})$$
$$c' \leftarrow c + \beta \mod p,$$

   and sends c' to EA.

4. EA records c' for c, computes $s' \leftarrow r + c'x \mod p$ and sends s' to c.

5. c checks if

$$[s']P = R' + [c']\mathsf{pk}^{\mathsf{EA}}_{\mathsf{Sch}},$$

   computes $s = s' + \alpha \mod p$ and EA's signature on $\mathsf{pk}^{\mathsf{c}}_{\mathsf{pec}} || \mathsf{pk}^{\mathsf{c}}_{\mathsf{sig}}$ is

$$\sigma_{\mathsf{c}} \leftarrow (R, s).$$

6. c sends $(\mathsf{pk}^{\mathsf{c}}_{\mathsf{pec}} || \mathsf{pk}^{\mathsf{c}}_{\mathsf{sig}}, \sigma_{\mathsf{c}})$ to the blockchain along with a signature on it signed using $\mathsf{sk}^{\mathsf{c}}_{\mathsf{sig}}$.

7. Nodes first verify the outer signature by $\mathsf{pk}^{\mathsf{c}}_{\mathsf{sig}}$, then checks if

$$[s]P = R + [c]\mathsf{pk}^{\mathsf{EA}}_{\mathsf{Sch}},$$

   where

$$c = \mathcal{H}(R, \mathsf{pk}^{\mathsf{c}}_{\mathsf{pec}} || \mathsf{pk}^{\mathsf{c}}_{\mathsf{sig}}).$$

   If only all of the checks are successful, nodes append the transaction to their ledger.

3.3. Testing

Before the testing stars, the exam authority randomly selects an examiner $\mathsf{e_c}$ for each candidate c and generates the test questions $\mathsf{q_c}$.

1. EA signs $(\mathsf{q_c}, \mathsf{pk_{e_c}})$, $\mathsf{S_{q_c}} \leftarrow \mathsf{S_{sig}}(\mathsf{sk_{ex}}, (\mathsf{q_c}, \mathsf{pk_c}, \mathsf{pk_{e_c}}))$.
2. EA encrypts $(\mathsf{pk_{e_c}}, \mathsf{S_{q_c}}, \mathsf{q_c}, \mathsf{pk_{e_c}})$ under $\mathsf{pk_c}$, i.e.
$$\mathsf{E_{q_c}} \leftarrow \mathsf{E_{pec}}(\mathsf{pk_c}, (\mathsf{pk_{e_c}}, \mathsf{S_{q_c}}, \mathsf{q_c}, \mathsf{pk_{e_c}})).$$
3. EA sends $\mathsf{E_{q_c}}$ to the blockchain along with a signature on it signed using $\mathsf{sk_{sig}^{EA}}$.
4. Nodes verify the outer signature by $\mathsf{pk_{sig}^{EA}}$. If successful, writes the transaction to the ledger.
5. c decrypts $\mathsf{E_{q_c}}$, i.e
$$(\mathsf{pk_{e_c}}, \mathsf{S_{q_c}}, \mathsf{pk_c}, \mathsf{pk_{e_c}}) \leftarrow \mathsf{D_{pec}}(\mathsf{sk_c}, \mathsf{E_{q_c}}).$$
6. c verifies $\mathsf{S_{q_c}}$ by checking that
$$1 = \mathsf{V_{sig}}(\mathsf{pk_{sig}^{EA}}, (\mathsf{q_c}, \mathsf{pk_{e_c}}), \mathsf{S_{q_c}}).$$
7. When c finishes her test, she appends her answers and her public key to the questions,
$$\mathsf{T_c} = (\mathsf{q_c}, \mathsf{pk_{e_c}}, \mathsf{a_c}, \mathsf{pk_c}).$$
8. c signs the filled test $\mathsf{T_c}$,
$$\sigma_\mathsf{c} \leftarrow \mathsf{S_{sig}}(\mathsf{sk_{sig}^c}, \mathsf{T_c}).$$
9. c encrypts $(\sigma_\mathsf{c}, \mathsf{T_c})$ under the public key of the stated examiner $\mathsf{e_c}$ and sends $\mathsf{E_{T_c}}$ to the blockchain along with a signature on it signed using $\mathsf{sk_{sig}^c}$.
$$\mathsf{E_{T_c}} \leftarrow \mathsf{E_{pec}}(\mathsf{pk_{pec}^{e_c}}, (\sigma_\mathsf{c}, \mathsf{T_c}))$$
10. Nodes verify the outer signature by $\mathsf{pk_{sig}^c}$. Then, they also verify that c completed the registration step[10]. If both checks are successful, writes the transaction to the ledger.

3.4. Marking

1. $\mathsf{e_c}$ decrypts $\mathsf{E_{T_c}}$ and gets
$$(\sigma_\mathsf{c}, \mathsf{T_c}) \leftarrow \mathsf{D_{pec}}(\mathsf{sk_{pec}^{e_c}}, \mathsf{E_{T_c}}).$$
2. $\mathsf{e_c}$ verifies the signature σ_c.
3. After marking the exam, the examiner $\mathsf{e_c}$ appends the mark $\mathsf{m_c}$ and generates
$$\mathsf{M_c} \leftarrow (\mathsf{T_c}, \mathsf{m_c}).$$

[10]The candidate can send Transaction ID belonging to the registration transaction

4. $\mathsf{e_c}$ signs $\mathsf{M_c}$ with his private key $\mathsf{sk}^{\mathsf{e_c}}_{\mathsf{sig}}$,

$$\sigma_{\mathsf{e,c}} \leftarrow \mathsf{S_{sig}}(\mathsf{sk}^{\mathsf{e_c}}_{\mathsf{sig}}, \mathsf{M_c}).$$

5. $\mathsf{e_c}$ encrypts $(\sigma_{\mathsf{e,c}}, \mathsf{M_c})$ for c and sends $\mathsf{E_{M_c}}$ to the blockchain along with a signature on it signed using $\mathsf{sk}^{\mathsf{e_c}}_{\mathsf{sig}}$.

$$\mathsf{E_{M_c}} \leftarrow \mathsf{E_{pec}}(\mathsf{pk}^{\mathsf{c}}_{\mathsf{pec}}, (\sigma_{\mathsf{e,c}}, \mathsf{M_c}))$$

6. Nodes verify the outer signature by $\mathsf{pk}^{\mathsf{e_c}}_{\mathsf{sig}}$. Then, they also verify that c completed the registration step[11]. If both checks are successful, writes the transaction to the ledger.

3.5. Notification

An eligible candidate c and the exam authority performs the notification phase together.

1. c decrypts $\mathsf{E_{M_c}}$ and gets $(\sigma_{\mathsf{e,c}}, \mathsf{M_c}) \leftarrow \mathsf{D_{pec}}(\mathsf{sk}^{\mathsf{c}}_{\mathsf{pec}}, \mathsf{E_{M_c}})$.

2. c verifies the signature $\sigma_{\mathsf{e,c}}$.

3. c creates a message

$$\mathsf{M} \leftarrow (\mathsf{M_c}, \sigma_{\mathsf{e,c}}, \mathsf{pk}^{\mathsf{c}}_{\mathsf{pec}} || \mathsf{pk}^{\mathsf{c}}_{\mathsf{sig}}, (\mathsf{R}, \mathsf{s}), \beta),$$

encrypts M for EA, and sends $\mathsf{E_M}$ to the blockchain along with a signature on it signed using $\mathsf{sk}^{\mathsf{c}}_{\mathsf{sig}}$,

$$\mathsf{E_M} \leftarrow \mathsf{E_{pec}}(\mathsf{pk}^{\mathsf{EA}}_{\mathsf{pec}}, M).$$

4. Nodes verify the outer signature by $\mathsf{pk}^{\mathsf{e_c}}_{\mathsf{sig}}$. Then, they also verify that c completed the registration step[12]. If both checks are successful, writes the transaction to the ledger. If successful, write the transaction to the ledger.

5. EA decrypts $\mathsf{E_M}$ and gets

$$(\mathsf{M_c}, \sigma_{\mathsf{e,c}}, \mathsf{pk}^{\mathsf{c}}_{\mathsf{pec}} || \mathsf{pk}^{\mathsf{c}}_{\mathsf{sig}}, (\mathsf{R}, \mathsf{s}), \beta) \leftarrow \mathsf{D_{pec}}(\mathsf{sk}^{\mathsf{EA}}_{\mathsf{pec}}, \mathsf{E_M}).$$

6. EA verifies the signature $\sigma_{\mathsf{e,c}}$ on $\mathsf{M_c}$ and also verifies (R, s) on $\mathsf{pk}^{\mathsf{c}}_{\mathsf{pec}} || \mathsf{pk}^{\mathsf{c}}_{\mathsf{sig}}$.

7. EA finds the candidate's identity using β and assigns the candidate's mark.

[11] The examiner can send Transaction ID belonging to the setup transaction.
[12] The candidate can send Transaction ID belonging to the registration transaction.

4. Performance and security discussion

Below, we give reasons why the properties of an online exam are satisfied assuming invigilation is in place.

- Test Answer Authentication. The exam authority encrypts the questions for the candidates who have pseudonyms signed by EA and only accepts marks whose signature can be verified by pseudonyms that have exam authority's signature on it. Since this signature can not be forged, test answer authentication property is satisfied.
- Examiner Authentication. Candidates encrypt their answers using the public key of the assigned examiner and this public key is signed by EA and EA only accepts marks whose signature can be verified by pseudonyms that have exam authority's signature on it. Since this signature can not be forged, examiner authentication property is also satisfied.
- Anonymous Marking. Since the examiner and the exam authority only knows the pseudonym of the candidate, anonymous marking property is satisfied. The exam authority can not associate the pseudonym of a candidate with the candidate's real identity since blind signature is used.
- Anonymous Examiner. Since the candidate only knows the pseudonym of the examiner that is going to mark that candidate's answers, anonymous examiner property is satisfied.
- Question Secrecy. The exam authority publishes the test questions after the candidates are under invigilation, so no candidate learns the test questions before the testing phase starts; hence, question secrecy holds.
- Question Privacy. Since test questions are encrypted with the candidate's pseudonym which does not link to the candidate's real identity, EA can not learn which test questions are assigned to a particular candidate. This guarantees question privacy.
- Mark Privacy. Mark privacy property requires that a candidate only learns her mark not the other candidates'. Since each mark is only carried encrypted under either the candidate's or the exam authority's public key, no one other than the candidate, the examiner that marked the exam, and the exam authority learns that candidate's mark.
- Test Verifiability. This property requires that both the exam authority and the candidate can verify that the mark given by the examiner is not changed. Since the mark is sent to the candidate by the examiner, candidate part is satisfied. Then, candidate sends the mark to the exam authority. Since this mark has signature of the examiner which is assigned to mark the test, the exam authority also is able to verify.

Please note that this scheme is not resistant to the situation where the exam authority and the candidate collude in any way. The exam authority may behave maliciously and give the exam questions to a specific candidate before the testing phase starts using other channels. Similar to the previously proposed schemes [4, 5, 7, 20], our scheme would suffer from this.

[4, 8–10] require full trust on exam authority. BSSSQS[13] only focuses on delivery of the test questions and [12–14] do not have marking and notification phases. There are four full e-exam proposals that do not rely on a trusted exam authority [2, 5, 7, 20], aside from this manuscript. [2] requires an administrator and candidates

[13] A. Islam, Md. F. Kader, and S. Y. Shin (2018). BSSSQS: A Blockchain Based Smart and Secured Scheme for Question Sharing in the Smart Education System [online]. Website https://arxiv.org/abs/1812.03917 [accessed January 2021].

to physically meet since they use visual cryptography in order to jointly generate candidates' pseudonyms. [20] is slightly modified version of [7] and both of them relies on exponential mix-nets for student and examiner anonymization and assume that "an authenticated, append-only, bulletin board is available. On it, everyone is guaranteed to see the same data. Write access will be restricted, however, to the appropriate entities ." Using blind signatures eliminates costly mix-net computations, and the described bulletin is exactly a permissioned blockchain. [5] does not satisfy test answer authentication, anonymous marking, anonymous examiner, and mark privacy properties as shown by [6].

Please note that from the five proposals that do not require a trusted exam authority, [2, 7] and we do not provide full security proofs, while [5, 20] verify their proposals using ProVerif [21].

Although we do not provide any implementation, Hyperledger Indy already supports verifiable credentials and can be used in our system for authentication purposes. Other than that, our system can work on Hyperledger Fabric[14].

5. Conclusion

In this manuscript, we proposed an online-exam scheme, which is based on verifiable credentials and blockchain. Since we used carefully chosen cryptographic primitives, our scheme achieves security and full privacy of the candidates/examiners. Candidates do not learn the questions or the identity of the examiner that marks their answers. Examiners do not know the identity of the candidate. The exam authority also does not know the link between the real identity of the candidates/examiners and their public keys. While satisfying these properties, we also ensure that only registered candidates and examiners take part in the exam. In addition, our scheme guarantees the secrecy of the candidate's mark from other candidates. It should be also noted that our scheme can be easily audited, since the data always remain unchanged due to the nature of blockchain.

We believe that registration phase can be realized without introducing other schemes, blind signatures in this case, using solely SSI concepts while satisfying anonymity of the candidates and also guaranteeing unique enrollment of a candidate. This remains as a future work.

Acknowledgment

Authors would like to thank the anonymous reviewers for their insightful comments.

References

[1] Ahmed FR, Ahmed TE, Saeed RA, Alhumyani H, Abdel-Khalek S et al. Analysis and challenges of robust E-exams performance under COVID-19. Results in Physics. Elsevier, 2021. doi: 10.1016/j.rinp.2021.103987

[2] Bella G, Giustolisi R, Lenzini G, Ryan PY. Trustworthy exams without trusted parties. Computers & Security. Elsevier, 2017. pp. 291-307. doi: 10.1016/j.cose.2016.12.005

[3] Catalano T, Gatti L. Representing teachers as criminals in the news: A multimodal critical discourse analysis of the Atlanta schools'"Cheating Scandal". Social Semiotics. Taylor & Francis, 2017. pp. 59-80. doi:10.1080/10350330.2016.1145386

[4] Castella-Roca J, Herrera-Joancomarti J, Dorca-Josa A. A secure e-exam management system. In: First International Conference on Availability, Reliability and Security; IEEE, 2006. doi:10.1109/ARES.2006.14

[14] Dmytro Bogatov (2020). Delegatable Anonymous Credentials Library [online]. Website https://github.com/dbogatov/dac-lib [accessed January 2021] is an example of such usage.

[5] Huszti A, Petho A. A secure electronic exam system. Publicationes Mathematicae Debrecen. Institutum Mathematicum, 2010. pp 299-312.

[6] Dreier J, Giustolisi R, Kassem A, Lafourcade P, Lenzini G et al. Formal analysis of electronic exams. In 2014 11th International Conference on Security and Cryptography (SECRYPT); IEEE, 2014. pp 1-12.

[7] Giustolisi R, Lenzini G, Ryan PY. Remark!: A secure protocol for remote exams. In: Cambridge International Workshop on Security Protocols; Springer, 2014. pp 38-48. doi:10.1007/978-3-319-12400-1_5

[8] Traoré I, Nakkabi Y, Saad S, Sayed B, Ardigo JD et al. Ensuring online exam integrity through continuous biometric authentication. In: Information Security Practices; Springer, 2017. pp 73-81. doi: 10.1007/978-3-319-48947-6_6

[9] Mitchell I, Hara S, Sheriff M. dAppER: decentralised application for examination review. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3); IEEE, 2019. pp 1-14. doi: 10.1109/ICGS3.2019.8688143

[10] Karthika R, Vijayakumar P, Rawal BS, Wang Y. Secure Online Examination System for e-learning. In: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE); IEEE, 2019. pp 1-4. doi: 10.1109/CCECE43985.2019.9052408

[11] Muzaffar AW, Tahir M, Anwar MW, Chaudry Q, Mir SR et al. A Systematic Review of Online Exams Solutions in E-Learning: Techniques, Tools, and Global Adoption. IEEE Access, IEEE, 2021. pp 32689-712. doi: 10.1109/ACCESS.2021.3060192

[12] Kausar S, Huahu X, Ullah A, Wenhao Z, Shabir MY. Fog-assisted secure data exchange for examination and testing in e-learning system. Mobile Networks and Applications. Springer, 2020. pp 1-7. doi: 10.1007/s11036-019-01429-x

[13] Sukadarmika G, Hartati RS, Sastra NP. Introducing TAMEx model for availability of e-exam in wireless environment. In: 2018 International Conference on Information and Communications Technology (ICOIACT); IEEE, 2018. pp 163-167. doi: 10.1109/ICOIACT.2018.8350741

[14] Mathapati M, Kumaran TS, Kumar AK, Kumar SV. Secure online examination by using graphical own image password scheme. In: 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM); IEEE, 2017. pp 160-164. doi: 10.1109/ICSTM.2017.8089144

[15] Giustolisi R, Lenzini G, Bella G. What security for electronic exams?. In: 2013 International Conference on Risks and Security of Internet and Systems (CRiSIS); IEEE, 2013. pp 1-5. doi: 10.1109/CRiSIS.2013.6766348

[16] Camenisch J, Drijvers M, Lehmann A. Anonymous attestation using the strong Diffie Hellman assumption revisited. In: International Conference on Trust and Trustworthy Computing; Springer, 2016. pp. 1-20. doi: 10.1007/978-3-319-45572-3_1

[17] Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth EuroSys conference; 2018. pp 1-15. doi: 10.1145/3190508.3190538

[18] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory. IEEE, 1985. pp 469-72. doi: 10.1109/TIT.1985.1057074

[19] Schnorr CP. Efficient identification and signatures for smart cards. In: Conference on the Theory and Application of Cryptology; Springer, 1989. pp 239-252. doi: 10.1007/0-387-34805-0_22

[20] Giustolisi R, Iovino V, Lenzini G. Privacy-Preserving Verifiability-A Case for an Electronic Exam Protocol. In: 2017 International Conference on Security and Cryptography (SECRYPT); 2017. pp. 139-150.

[21] Blanchet B. Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif. In: Alessandro A (editor). Foundations of Security Analysis and Design VII: FOSAD 2012/2013 Tutorial Lectures. Cham: Springer International Publishing, 2014, pp 54-87.