PREVENTING FORGED AND FABRICATED ACADEMIC CREDENTIALS USING CRYPTOGRAPHY AND QR CODES

Cheman Shaik

VISH Consulting Services Inc, 6242 N Hoyne Avenue, Chicago IL 60659, USA

ABSTRACT

Theobjective of this paper is to present a method of detecting forgery and fabrication in educational certificates and academic transcripts based on cryptography and QR codes. Discussed in detail are the requirements that need to be met by educational institutes issuing academic certificates or transcripts. The cryptographic steps of converting certificate details into a ciphertext, encoding it in a QR code and printing the same on the certificate or transcript to be issued are elaborated. This paper also explains in detail how the certificate owners, other institutes, employers and third-party verifiers can verify certificates for forgery and fabrication using the scanning app of the issuing institute. The encryption and decryption formulae that should be used in computations to be performed before creating and after scanning a QR code are documented. Educational institutes and universities can implement this method in their certificate issuing process just by obtaining a cryptographic key pair and publishing their QR code scanning app for download by verifiers.

KEYWORDS

Educational Certificate, Transcript, Forgery Detection, Cryptography, Encryption, Decryption, Public Key, Private Key, QR Code. Mobile App, Desktop App

1. INTRODUCTION

Fraudulent academic credentials, including forged and fabricated degree certificates and transcripts, are a growing concern all over the world affecting institutions, universities, employers, and even education loan offering banks. Such fraudulent credential holders seriously affect the brand image of the higher institutions they are admitted to and the productivity of the organizations they are hired by.

The level of forgeries practiced by miscreants varies from small high school diplomas to doctorates, using which admissions are sought into higher institutions or even foreign universities. Illegal Agencies offering forged diplomas and degrees are wide spread in certain Asian and African countries. There is no fool-proof mechanism for the spot detection of forgery and fabrication in an academic credential, other than referring it to the institute the certificate claims to have been issued by, which is very time consuming and may take up to weeks.

Professional forging agencies create forged certificates for a price using the image editing software, Photoshop and high-resolution color printers. As per a CNN report, a board member of the Council for Higher Education Accreditation estimated that more than 100,000 fake degrees are sold each year in the U.S. alone [1].

There are lot of educational certificate verification service agencies who provide their service for a fee. They contact the college, university, or school that issued the degree or certificate for

DOI: 10.5121/ijcsea.2021.11102

verification. Most of the credentials are verified by the institute's Admissions and Records Office. However, such a verification process is subject to delays or even result into no output as some institutions prohibit access to their records to people other than their previous students [2].

Recently, there has been lot of brain storming ongoing to consider blockchain technology in the education sector. However, blockchain implementation throws several challenges to educational institutes, such as standardization, governance and dependencies on third parties [3].

2. RELATED WORK

Proposals were made in the past to build blockchain networks for decentralized logging of educational credentials. In 2017, Muhamed Turkanović et al proposed a global higher education credit platform, named EduCTX, which is a higher education credit, and grading system that can offer a globally unified viewpoint for students and higher education institutions, companies, institutions, and organizations [4].

In 2017, the Japanese firm Sony announced that they developed a commercial digital system for storing and managing educational records such as diplomas, degrees and tests on the blockchain [5].

In 2018, Arenas et al discussed the application of permissioned blockchain in education, specifically for verification of academic credentials by various interested education stakeholders and relevant third parties to access data of candidates [6].

In 2019, Omar et al proposed a blockchain based framework for verifying educational certificates focusing on themes including authentication, authorization, confidentiality, privacy and ownership. They also identified the gaps and loopholes in the current blockchain based educational certificate verification solutions [7].

In 2019, Melissa Rizzi published a list of signs to look out for in forged documents. The list of signs includes misaligned printing, incorrect fonts, pixelated signatures, use of inappropriate language, mismatching registrar name, outdated university name and illegitimate awarding body [8].

All the technical work mentioned above is related to the blockchain approach to recording and verification of educational certificates. However, blockchain is still in its infancy and has go a long way before its maturity and standardization in the education sector.

No evidences are found in literature of using a blend of cryptography and QR codes for detecting forgery and fabrication in educational certificates.

3. CRYPTOGRAPHY

Cryptography is a mathematical technique that converts the original data in to an illegible content making no sense to its unintended readers [9]. The converted data is produced by running on the original data an algorithm with a key in encryption or without a key in hashing [10].

Basically, encryption can be classified into two categories – symmetric key encryption that uses a single key for both encryption and decryption, and asymmetric key encryption that uses two different keys, one for encryption and another for decryption. Advanced Encryption Standard (AES) uses the symmetric key encryption while RSA (Rivest, Shamir, Adleman) and ECC (Elliptic Curve Cryptography) fall under the asymmetric key encryption category [11].

Asymmetric Key Cryptography, also called Public Key Cryptography, uses a public key to encrypt the original data anda private key to decrypt the encrypted data. The encrypted data is called ciphertext. The public and private keys are mathematically related but deriving one from the other is practically infeasible as the computational effort required is enormous even if carried over a cluster of super computers [12].

4. QR CODES

QR Code is a two-dimensional matrix, mostly square shaped, that can encode large amount of data in byte, numeric and alphanumeric form. A QR Code can be decoded by a handheld scanner or a QR Code scanner mobile app installed on a smartphone or desktop. A QR Code can store up to 7,089 numeric characters or 2,953 alphanumeric characters [13].

Every QR Code is surrounded by a thick white border called quiet zone to differentiate the QR Code image from its background images. The encoding region contains format information, version information, data and error correction codes. Three position markers positioned at the corners except the bottom right corner guide cameras and scanners to locate data modules and the scanning direction[14].

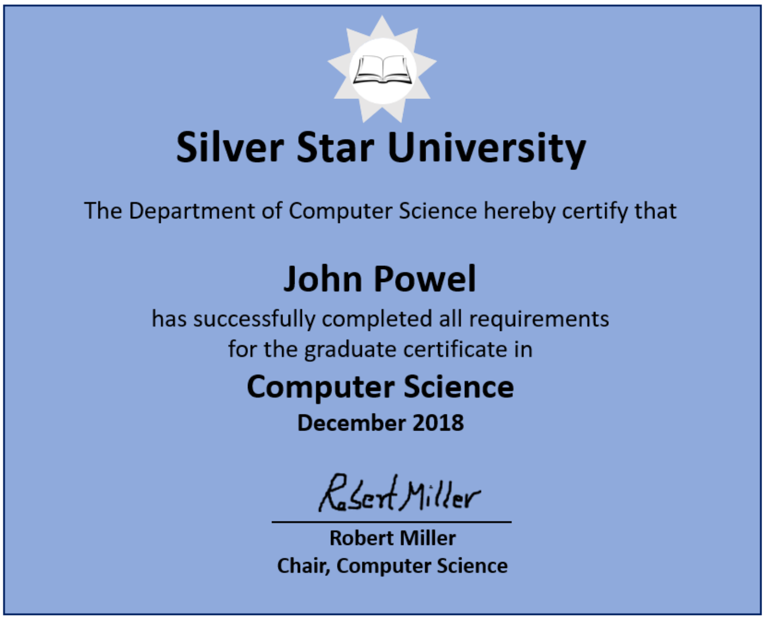
QR Codes are useful several ways such as to connect to Facebook profiles, direct users to social media accounts, share audio/video files, send text in any language, connect to websites and so on[15].

5. APPLYING CRYPTOGRAPHY AND QR CODES

In this section, we present a method in which forged and fabricated certificates and transcripts can be detected by applying a blend of cryptography and QR code technologies. In order to make it possible, every institution that issues certificates and transcripts to its students should obtain a public and private key pair of any cryptosystem. The public key must be published on their website in the form of QR Code. A public key in the form of QR Code facilitates its easy scanning and integration by certificate and transcript verifiers in the institute’s mobile and desktop scanning applications. The institution also needs to create and publish a QR code scanning app on their website for download by certificate verifiers. The institute should store its publc key in the scanning application’s memory. The scanning app should be capable of performing decryption of the content encoded in the QR codes printed on their certificates.

Further, the institution or the university issuing academic certificates and transcripts should encrypt their content with the private key and encode the ciphertext in a QR code which should be printed on the academic certificate or transcript issued to the student. Any verifier who wants to verify the certificate of transcript can download the institute’s QR code scanning application from the institute’s website and scan the QR code on the certificate or transcript. When the verifier focusses the device camera on the QR code, the scanning application grabs the information encoded in the QR code and decrypts it with the public key saved in the application’s memory and displays the information on the device screen. As the information encoded in the QR code is in encrypted form, it needs to be decrypted with the institute’s public key stored in the scanning application’s memory, which will generate the actual information printed on the certificate. The verifying party should verify this generated information with the information on the hard copy of the certificate or transcript. Any mismatch of the information is a clear indication of forgery.

Fig. 1 below shows an example certificate issued to a student by a university without a QR code as per the current practice in the education sector. Such a certificate provides no technical means to verify its authenticity and detect forgery or fabrication.



Silver Star University

The Department of Computer Science hereby certify that

John Powel

has successfully completed all requirements
for the graduate certificate in

Computer Science

December 2018

Robert Miller

Robert Miller
Chair, Computer Science

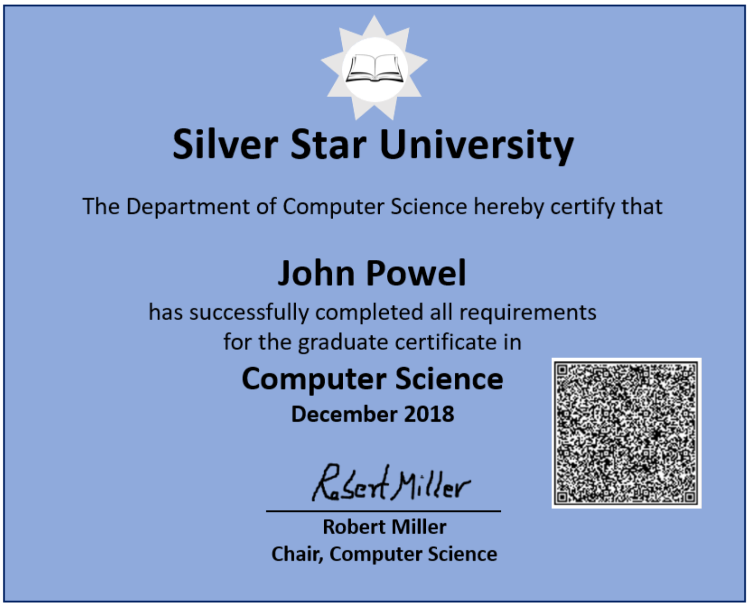
Fig.1 An example Degree Certificate issued by a University

Before issuing a print command to a printer to print the certificate, the university's software application captures all the fields of the certificate such as the university name, student name, degree awarded, month and year of award, department and specialization and the signing authority. The application retrieves the university's private key from its database or a protected folder and encrypts with it the captured data and encodes the ciphertext in a QR Code. Table.1 below shows the information captured and the QR Code encoding encrypted information.

Table 1. A certificate information and the QR code encoding the ciphertext

Student Certificate Information Captured	QR Code
University: Silver Star University Department: Computer Science Student: John Powel Degree: Graduate Specialization: Computer Science Month and Year: December 2018 Signed By: Robert Miller, Chair, Computer Science	

The printed certificate bearing the QR code is issued to the student. Fig. 2 below shows the same certificate issued with the QR code printed on it.



Silver Star University

The Department of Computer Science hereby certify that

John Powel

has successfully completed all requirements
for the graduate certificate in

Computer Science

December 2018

Robert Miller

Robert Miller
Chair, Computer Science

Fig.2 An example Degree Certificate with QR code issued by a University

6. Mobile and Desktop Application to Verify Authenticity

Every educational institute and university issuing certificates with encrypted QR codes should develop and publish a scanner application on their website, Google Play Store or Appstore for download to enable students and third parties scan their issued certificates. The app should have their public key stored in its memory. It also provides a button to open the device camera to scan the QR code on a certificate. When the camera id focused on the QR code, the app performs verification in two steps, first it captures the encoded ciphertext in the QR code, next it decrypts the captured ciphertext into a plain text using the public key stored in its memory and displays the information on the device screen. The verifying party can compare the plain text with the actual printed content on the certificate. Any mismatch between the two proves forgery or fabrication of the certificate. Table.2 below shows the screenshot of the app scanning the QR code on a certificate and the retrieved plain text information pertaining to the certificate.

Table 2. A third-party verification of QR code on an academic certification

QR Code Scan of Certificate	Certificate Information Derived on Decrypting QR Code Ciphertext
 nith d all requirements rtificate in cience 018 ller ler Science	University: Silver Star University Department: Computer Science Student: John Powel Degree: Graduate Specialization: Computer Science Month and Year: December 2018 Signed By: Robert Miller, Chair, Computer Science

Scanning a QR code with any general QR code scanner apps will retrieve only the encoded ciphertext from the QR code. The QR code scanner app needs to have the additional cryptographic functionality built into it in order to decrypt the encoded ciphertext using the public key of the certificate issuing authority.

Encrypted QR codes provide a light weight, low cost solution to detect forgery and fabrication in educational certificates and transcripts compared to the blockchain solution. Encrypted QR codes can be implemented with a very nominal cost to academic institutes and absolutely no cost to students and third-party verifiers.

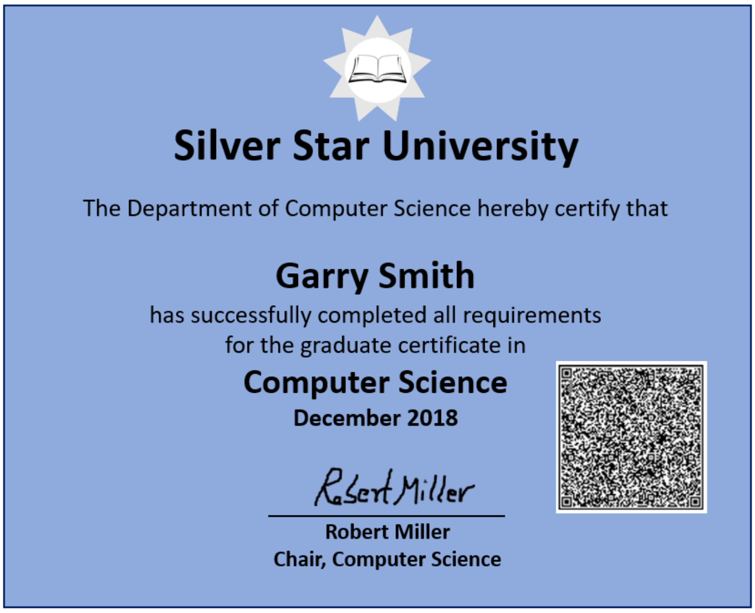
7. A Universal Mobile App for All Institutions

Download and install of QR code scanning apps of several institutions, especially by large universities during admissions and corporate companies during mass recruitments could be very time consuming. A universal mobile app may be developed and placed on Google Play Store and iPhone App Store. The universal app may provide UI screens to add different institutes and their corresponding public keys to the app memory. When a certificate verifier wants to scan a certificate, he can select the institute issuing the certificate from the existing list and focus the camera over the QR code which would capture and decrypt the ciphertext encoded therein with the public key of the institute.

Academic institutes world wide could publish their public keys on their respective websites in the form of QR code so it would be easy to capture and store them with the scanning app. Another, better approach is to release the initial version of the app with the public keys of most popular institutes and universities around the word built into it to avoid time consuming visits to all their websites by verifying parties. Any missing institutes could be allowed to join the app later through online registration. The additional institutes may be added to the already installed app through over-the-air data updates. Alternatively, app users could integrate any missing institutes and universities manually as required.

8. QR Code Scan Output of Forged Certificates

When a forger or fabricator alters or completely replaces the content in a genuine certificate with QR code, he has two options, either leaving the QR code as is or replacing the actual QR code with his own QR code encoding the altered or replacing information encrypted with his own private key. Fig.3 below shows a forged certificate leaving the QR code as is.



Silver Star University

The Department of Computer Science hereby certify that

Garry Smith

has successfully completed all requirements
for the graduate certificate in

Computer Science

December 2018

Robert Miller

Robert Miller
Chair, Computer Science

Fig.3 An example forged Degree Certificate with QR code

Table. 3 below shows content obtained on scanning the QR code and the content printed on the forged certificate.

Table 3. Content obtained on QR code scan and content on the forged certificate

Content from QR Code Scan	**Content on Certificate Hard Copy**
University: Silver Star University Department: Computer Science Student: **John Powel** Degree: Graduate Specialization: Computer Science Month and Year: December 2018 Signed By: Robert Miller, Chair, Computer Science	University: Silver Star University Department: Computer Science Student: **Garry Smith** Degree: Graduate Specialization: Computer Science Month and Year: December 2018 Signed By: Robert Miller, Chair, Computer Science

As the student name from QR code scan result mismatches with the one printed on the certificate, it is a clear indication of forgery.

On the other hand, if the forger prints his own QR code that he generated encoding the printed information using his own private key, it will produce a totally junk text on the QR code scan by a verifier, which will again prove forgery of the academic certificate. This is because the forger's private key and the institute's public key stored in the app memory are not mathematically related to produces an exactly matching content to escape forgery detection.

9. Certificate Encoding into QR Code

Forgery verification of academic certificates can be implemented using any public key crypto system. Today, the industry standard for RSA key length is 2048 bits. With RSA encryption, the plain certificate information M is encrypted to generate a ciphertext C as shown below:

$C = M^e \bmod n$, where e is the private key exponent and should be kept secret.

The ciphertext C is encoded into a QR code that should be printed on the certificate.

When the QR code scanning app of the institute scans the QR code, it will capture the ciphertext C from it and decrypt it to the original plain text M as shown below:

$M = C^d \bmod n$, where d is the public key exponent stored in app memory

The key modulus n is common on both sides and should be stored in memory of both the certificate printing and scanning applications.

In public key cryptography use cases of ecommerce and online communication, usually the plain text is encrypted with the public key and the ciphertext is decrypted with the private key. However, in this case the process is reversed, that is, the plain text is encrypted by the private key and the ciphertext is decrypted with the public key.

10. Precautions on Selecting the Public Key

Usually, small numbers like 3 or 65537 are chosen as the encrypting exponent of an RSA key in order to minimize the ciphertext computation effort. This practice should be unfollowed for generating keys for QR code verification of educational certificates and transcripts. The encrypting key exponent should be the order of the key modulus. Otherwise, it can minimize a brute force attacker’s effort in guessing the right exponent that would generate the right QR code to be printed on the forged certificates and transcripts to escape forgery detection.

11. BENEFICIARIES OF THE TECHNIQUE

Encrypted QR code certificates will be useful to a multitude of beneficiaries including:

- students who like to scan their own certificates
- institutes offering admissions to higher degrees courses for qualifying students with lower degrees
- universities offering admissions to native as well as foreign students
- employers and recruiters offering jobs based on qualifications
- third parties offering certificate verification and attestation services
- immigration authorities
- government agencies conducting competitive examinations
- banks offering student loans

12. PRACTICAL IMPLEMENTATION AND ADOPTION

Adoption of encrypted QR Code certificates will spread rapidly once open-source mobile apps are developed and educational institutes start issuing certificates with encrypted QR codes to their passing students. The cost incurred by an institute or university would be very nominal as it requires them only to acquire a cryptographic key pair and publish their public key on their website.

Education ministries around the word may release policies mandating their academic institutes and universities to printencrypted QR code on their certificates. An open-source trusted app that can integrate and manage the public keys of institutes around the world will become a great thrust for the adoption of QR coded certificates. Education ministries, universities, or large software companies may take the initiative to develop and release such mobile and desktop apps to help QR coded certificates evolve as a standard of the education industry. Also, branded mobile phones may include such an app in their built-in apps provided with the device.

13. ENCRYPTED QR CODES VS BLOCKCHAIN

Of late blockchain technology is finding application in a wide range of sectors including education. However, blockchain is a very complicated leger that brings lot of challenges and burdens along with its advantages. Every small institute may not be able to afford products and services based on the blockchain technology. Moreover, the growth of a blockchain ledger is tied to the incentives provided for miners for solving a cryptography puzzle that would add a new block to the leger. It is more suitable for financial and other such sectors where there is lot of money spinning around.

On the other hand, encrypted QR codes provide a very light weight solution for forgery and fabrication detection in educational certificates which brings only a nominal cost to the academic institutes and universities and zero cost and burden to students and third-party verifiers. Forgery detection can be done with both hard copy certificates as well as their digital copies.

14. CONCLUSION

Certificate forgery is a serious concern for educational institutes, universities, employers, organizations, immigration authorities and even government departments as it affects the opportunities of those who earn educational degrees with sustained hard work throughout their course duration. It also degrades the education standard of the society and affects productivity of the organizations hiring the candidates holding such forged degrees.

A new method of detecting forgery in academic credentials using cryptography and QR codes has been presented. Explained in detail is the procedure of encrypting a certificate content to produce a ciphertext, creating a QR code encoding the ciphertext and printing it on the certificate to be issued. Also explained in detail is how a mobile or desktop app can integrate the public key of the institute issuing the certificate and scan it for forgery and fabrication.

The proposed method requires that academic institutes and universities obtain a cryptographic key pair and also develop and publish a scanning app using which certificate verifiers can scan the encrypted QR code on their issued certificates. It is also recommended that an opensource mobile and desktop application be developed and placed on the web for download, which will relieve the institutes from the burden of developing their own independent scanning apps.

QR coded certificates may be implemented very easily with minimal cost to academic institutes and universities. These certificates enable quick detection of forgery and fabrication by the verifying students, institutes, universities, employers, immigration authorities, banks and third parties offering certificate verification services.

REFERENCES

[1] Embry-Riddle Aeronautical University, "Fraudulent Transcripts", https://commons.erau.edu/cgi/viewcontent.cgi?article=2490&context=publication

[2] exactbackgroundchecks.com, "Education Verification", “https://www.exactbackgroundchecks.com/education-verification.html

[3] Alexander Grech and Anthony F. Camilleri , “Blockchain in Education”, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf

[4] M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," in IEEE Access, vol. 6, pp. 5112-5127, 2018, doi: 10.1109/ACCESS.2018.2789929.

[5] Jon Russell, “Sony wants to digitize education records using the blockchain”, https://techcrunch.com/2017/08/09/sony-education-blockchain/

[6] R. Arenas and P. Fernandez, "Credence Ledger: A Permissioned Blockchain for Verifiable Academic Credentials," 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, 2018, pp. 1-6.

[7] OMAR S. SALEH, OSMAN GHAZALI, MUHAMMAD EHSAN RANA, "BLOCKCHAIN BASED FRAMEWORK FOR EDUCATIONAL CERTIFICATES VERIFICATION", Journal of Critical Reviews, Vol 7, Issue 3, 2020

[8] Melissa Rizzi, "An Answer to University Document Fraud", https://www.digitary.net/answer-to-doc-fraud/

[9] Kevin Stine and Quynh Dang, "Encryption Basics", http://library.ahima.org/doc?oid=104090#.X_6MluhKhPY

[10] SSL2BUY.com, "Difference Between Hashing and Encryption", https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption

[11] NICOLAS POGGI, "Types of Encryption: Symmetric or Asymmetric? RSA or AES?", https://preyproject.com/blog/en/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes/

[12] docstore.mik.ua,"ACryptographyPrimer", https://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch03_02.htm

[13] Scanova Blog, "What is a QR Code: A Beginner’s Guide", https://scanova.io/blog/what-is-a-qr-code/

[14] Sumit Tiwari, "An Introduction To QR Code Technology", 2016 International Conference on Information Technology

[15] QR Code Generator, "How Does a QR Code Encode Data?", https://www.qr-code-generator.com/blog/how-does-a-qr-code-encode-data/

AUTHOR

Cheman Shaik is a Research & Development professional in Computer Science and Information Technology for the last twenty years. He has been an inventor in these areas of technology with eight U.S Patents for his inventions in Cryptography, Password Security, Codeless Dynamic Websites, Text Generation in Foreign Languages, Anti-phishing Techniques and 3D Mouse for Computers. He is the pioneer of the Absolute Public Key Cryptography in 1999. He is well known for his Password Self Encryption Method which has earned him three U.S Patents. He has published research papers in the international journals – IJCSEA, IJCIS and the proceedings of EC2ND 2006 and CSC 20

DISCLAIMER

The educational certificate used in this paper is not a real one issued to any real student but a prepared one only for the purpose of illustration.