Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 6, Issue 3, March-2019

# EXAMINATION SECURITY USING QR CODE

P Matan[1], R Ravichandran[2], C Varun Raman[3] ,V Gokula Krishnan[4]

[1]UG Scholar, Department of Computer Science and Engineering, Panimalar Institute of Technology,Chennai, Tamil Nadu, India

[2]UG Scholar, Department of Computer Science and Engineering, Panimalar Institute of Technology,Chennai, Tamil Nadu, India

[3]UG Scholar, Department of Computer Science and Engineering, Panimalar Institute of Technology,Chennai, Tamil Nadu, India

[4]Associate Professor, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, Tamil Nadu, India

*Abstract* —***The chance of the question paper getting leaked is increasing day by day and a solution is proposed to solve this problem. Elliptic Curve Cryptography (ECC) along with QR code will be a solution to this problem. QR code (Quick Response) is the trademark for a type of matrix (two dimensional) barcode. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary and kanji) to store data efficiently. Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. ECC technique involves conversion of text to cipher text. The cipher text is then converted to a QR Code. During decryption, the QR code is scanned and the content is decrypted. Only the application can read the original data shared in QR code since the data is encrypted with ECC with the integrity being maintained. An additional feature of linking the student's answer sheet with hall ticket and question paper is also added to avoid paper frauds and making re-evaluation a simpler task. Once the evaluation is done, the examiner can then scan the code and enter the mark in the student database which is maintained by the university.***

***Keywords-QR Code, ECC, RSA, DES, Encryption, Decryption.***

## I. INTRODUCTION

*In this age of the digital era, with the progress of technology and continuous growth in digital data, there is an important need of optimization of data and information presently in the digital world. The authenticity of data is the trickiest issue in management of data in the internet database. In order to achieve this, we use cryptography.*

*Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. Cryptography allows people to keep confidence in the electronic world. People can do their business on electric channel without worrying of deceit and deception. Confidentiality, data integrity, authentication, and non-repudiation are central to cryptography. Modern cryptography exists in almost every disciplines like mathematics, computer science and electrical engineering. Cryptography involves two methods called encryption and decryption. Encryption changes the plain text to cipher text using encryption algorithms such that no one other than the sender can make sense out of it using a key generated by the algorithm during the encryption process. Decryption is the reverse of encryption that is done on the receiving end. But in order to do it the receiver must have the knowledge of key otherwise he will not be able to make sense out of the received encrypted message.*

*In this, we mainly consider the problem of exam papers getting leaked. Keeping this problem in mind, we have introduced a new digital documentation system using QR codes. QR Code is a type of 2 dimensional matrix barcode, which is more popular than 1-D barcodes because of its large capacity of digital data and it can be readable in any mobile devices. By combining Elliptical Curve Cryptography with QR code, we can achieve a new level of reliable communication.*

## II. EXISTING SYSTEM

All previous visual cryptography schemes were only limited to binary images. These techniques were capable of doing operations on only black and white pixels. It is not sufficient for real life applications. In this scheme a dithering technique is used to convert gray level image into approximate binary image. Then existing visual cryptography schemes for binary images are applied to create the shares. In RSA algorithm, the key size is very big and generates longer cipher texts and signatures. Even the key generation is slow and the two-part key in RSA is very vulnerable to attacks.

## III. PROPOSED SYSTEM

Before the QR code is generated from the question paper, the question paper is encrypted using Elliptical Curve Cryptography (ECC). ECC is preferred over RSA due to the lesser size of the keys and provides the same amount of security. ECC can provide the same security with 164-bit key that RSA systems provide with 1024- bit key. It is mostly useful for mobile applications as it has the capability to provide high level security with low computing power and battery resource.

## IV. ALGORITHMS USED

In this application, two algorithms are used namely, ECC and QR code generation.

### 4.1 Elliptical Curve Cryptography

Elliptical curve cryptography is a public key encryption technique which is based on the theory of elliptical curves. This encryption technique uses the properties of elliptic curve in order to generate keys instead of using the traditional methodology of generation of keys using the product of two very large prime numbers. The most important advantage of elliptical curve cryptography is the use of smaller keys providing the same level of security. ECC can provide the same security with 164-bit key that other systems provide with 1024- bit key. ECC is a public key cryptosystem which is used to generate the public key and the private key in order to encrypt and decrypt the data. It is based on the mathematical complexity of solving the elliptic curve discrete logarithm problem which deals with the problem of calculating the number of steps or hops it takes to move from one point to another point on the elliptic curve.

Elliptic curves are the binary curves and are symmetrical over x- axis. These are defined by the function:

$$y^2 = x^3 + ax + b$$

where x and y are the standard variables that define the function while as a and b are the constant coefficients that define the curve .As the values of a and b change, elliptical curve also alters.

**Steps involved in ECC Algorithm**

ECC is a public key cryptosystem where every user possesses two keys: public key and private key. Public key is used for encryption and signature verification while as private key is used for decryption and signature generation.

**Key Generation**

It is the most important step in which an algorithm is used to generate both private and public keys. Sender encrypts the message data with the help of receiver's public key and receiver decrypts the data using its private key.

Step 1 – Thesender selects a random number sA between the range [1 , n-1].This is the private key of the sender.
Step 2 – Thenthe sender generates the public key using the formula PA = sA*G
Step 3 – Similarlyreceiver selects a private key sB and generates its public key
PB =sB*G.
Step 4 – Thesender generates the security key "K=sA*PB" and the receiver also generates the security key "K= sB*PA"

**Signature Generation**

To sign a message m by the sender, it performs the following steps

Step 1 – Itcalculates a cryptographic hash function
Step 2 – Thesender then selects a random integer k from [1,n-1]
Step 3 – The it computes a pair (r,s)
Step 4 – r=x1(mod n ) where (x1,y1) =k*G
Step 5 – s= k-1(e+ sA*r)
Step 6 – Thispair (r,s) defines the signature
Step 7 – Thissignature is sent to the receiver.

**Encryption**

Suppose sender wants to send a message m to the receiver

Step 1 – Letm has any point M on the elliptic curve
Step 2 – Thesender selects a random number k from [1,n-1]
Step 3 – Thecipher texts generated will be the pair of points(B1,B2) where
B1= k*G
B2= M + (k*G)

**Decryption**

To decrypt the cipher text, following steps are performed

Step 1 – Thereceiver computes the product of B1 and itsprivate key
Step 2 – Thenthe receiver subtracts this product from thesecond point B2
M = B2- (sB * B1)
M is the original data sent by the sender

**Signature Verification**

To authenticate the sender's signature, the receiver must have the knowledge about sender's public key PA

Step 1 – Forauthentication the receiver needs to verify the pair (r,s) are in the range of [1,n-1]
Step 2 – Thereceiver again then calculates the hash function e as in signature generation
Step 3 – Thenthe receiver calculates w =s-1 mod(n)
Step 4 – Thencalculate u1= e*w (mod n) and u2 = r*w (mod n)
Step 5 – Calculate(x1,y1)= u1*G + u2*PA
Step 6 – Ifx1 = r (mod n), then the signature is valid.

### 4.2 QR Code Generation

The algorithm consists of 7 steps:

Step 1: Data Analysis

The QR standard has four modes for encoding text: numeric, alphanumeric, byte, and Kanji. Each mode encodes the text as a string of bits (1s and 0s), but each mode uses a different method for converting the text into bits, and each encoding method is optimized to encode the data with the shortest possible string of bits. Therefore, the first step should be to select the most optimal mode for your text.

Step 2: Data Encoding

Now that you have selected the appropriate encoding mode for your text, the next step is to encode the text. The data encoding section describes this process in detail for each encoding mode. The result of this step is a string of bits that is split up into data codewords that are each 8 bits long.

Step 3: Error Correction Coding

QR codes use error correction. This means that after we create the string of data bits that represent your text, we must then use those bits to generate error correction code words using a process called Reed-Solomon error correction.

Step 4: Structure Final Message

The data and error correction codewords generated in the previous steps must now be arranged in the proper order. For large QR codes, the data and error correction codewords are generated in blocks, and these blocks must be interleaved according to the QR code specification.

Step 5: Module Placement in Matrix

After generating the data codewords and error correction codewords and arranging them in the correct order, you must place the bits in the QR code matrix. The codewords are arranged in the matrix in a specific way.

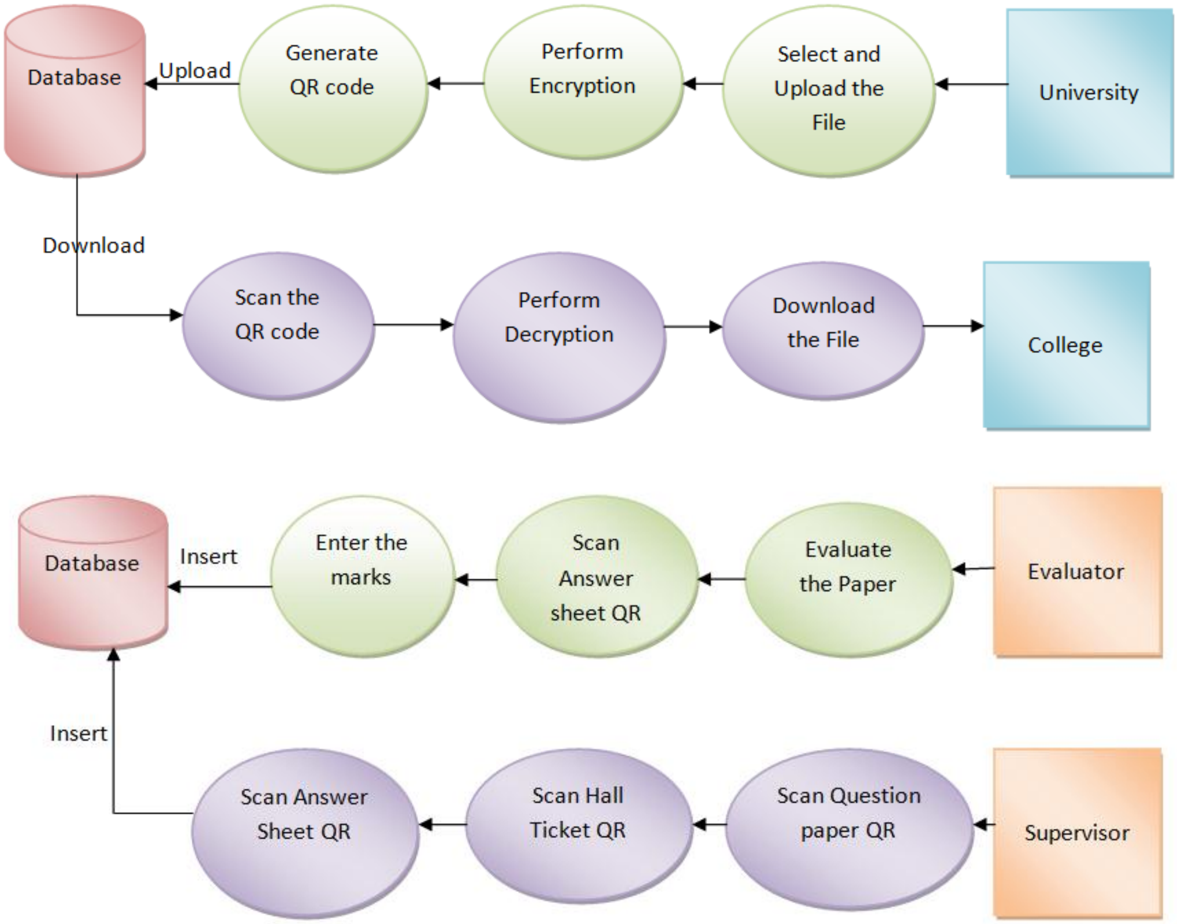
Step 6: Data Masking

Certain patterns in the QR code matrix can make it difficult for QR code scanners to correctly read the code. To counteract this, the QR code specification defines eight mask patterns, each of which alters the QR code according to a particular pattern. Determining which of these mask patterns results in the QR code with the fewest undesirable traits is done by evaluating each masked matrix based on four penalty rules.

Step 7: Format and Version Information

The final step is to add format and (if necessary) version information to the QR code by adding pixels in particular areas of the code that were left blank in previous steps. The format pixels identify the error correction level and mask pattern being used in this QR code. The version pixels encode the size of the QR matrix and are only used in larger QR codes

## V. WORKING OF THE SYSTEM



### 5.1 University Login

This is the module where the question paper gets uploaded to the cloud servers. Only the administrator can login and do these operations with a unique set of credentials. The steps are as follows.

1. The administrator logs in with the username and password.
2. The question paper which is in a PDF format is selected from the phone’s storage.

3. Next, the subject code and question paper code is entered by the administrator.
4. After submitting the details, the paper gets uploaded into the cloud storage and the question paper details are inserted into the database along with the location of the question paper file.
5. When the file is uploaded, a QR code is generated by the application and the administrator can share the code with the other institutions.

### 5.2 College Login

This is the module where the question paper is retrieved by the college at the specified time only. Each college has a unique set of credentials.

1. The college can login with their credentials and then request the question paper for the corresponding exam.
2. Do note that, downloading the file is only possible only 2hours before the exam starts.
3. The users should scan the QR code, get the link and then download the question paper.
4. If there are multiple exams, all the QR codes must be scanned individually.
5. If time has lapsed or if it is too early, the link will not be generated.

### 5.3 Supervisor Login

This is the login that is used by the hall supervisor. Every supervisor has his/her credentials. The role of the supervisor is to enter the student's details in the database.

1. The supervisor first logs in with the credentials.
2. Then 3 different scanners are provided to scan the QR code from the question paper, hall ticket and answer sheet.
3. After all 3 codes are scanned, a new row is inserted into the result database and a dummy number is generated and the mark field is left empty.
4. This is done to check the attendance of the student as well.

### 5.4 Evaluator Login

This login is for the evaluator, the people who check the answer sheet and enter the marks for the answer sheet.

1. The evaluator logs into the application.
2. The QR code on the answer sheet is scanned by the supervisor and the mark is entered for that particular student.

## VI. CONCLUSION

In this paper, we are able to bring a solution to the question paper getting leaked. We are able to encrypt the question paper using Elliptical Curve Cryptography and make it into a QR code. There is no data loss at all and complete integrity of the file is maintained throughout the process. Additionally, we are able to access the question paper only 2 hours in prior to the exam and not before that, thereby preventing any chances of leaking. We are also able to track the student's attendance for the exam and have made it possible for the evaluator to enter the marks a very easy process.

## REFERENCES

[1] M. Naor and A. Shamir, ‘‘Visual cryptography,’’ in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 950, A. De Santis Eds. Berlin, Germany: Springer-Verlag,May 1995,pp. 1–12.

[2] C.-N. Yang and D.-S. Wang, ‘‘Property analysis of XOR-based visual cryptography,’’ IEEE Trans. Circuits Syst. Video Technol., vol. 24, no. 2, pp. 189–197, Feb. 2014.

[3] G. Shen, F. Liu, Z. Fu, and B. Yu, ‘‘Perfect contrast XOR-based visual cryptography schemes via linear algebra,’’ Des. Codes Cryptogr., vol. 85, no. 1, pp. 15–37, Oct. 2017.

[4] S. J. Shyu and M. C. Chen, ‘‘Minimizing pixel expansion in visual crypto- graphic scheme for general access structures,’’ IEEE Trans. Circuits Syst. Video Technol., vol. 25, no. 9, pp. 1557–1561, Sep. 2015.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, ‘‘Visual cryptography for general access structures,’’ Inf. Comput., vol. 129, no. 2,pp. 86–106, Sep. 1996.[6] S. Arumugam, R. Lakshmanan, and A. K. Nagar, ‘‘On (k, n)∗-visual cryptography scheme,’’ Des., Codes Cryptogr., vol. 71, no. 1, pp. 53–162,Apr. 2014.

[7] S. Sridhar, R. Sathishkumar, and G. F. Sudha, ‘‘Adaptive halftoned visual cryptography with improved quality and security,’’ Multimedia Tools Appl., vol. 76, no. 1, pp. 815–834, Jan. 2017.

[8] C.-N. Yang, L.-Z.Sun, and S.-R.Cai, ‘‘Extended color visual cryptography for black and white secret image,’’ Theor. Computer. Sci., vol. 609,pp. 143–161, Sep. 2016.

[9] H. Hu, G. Shen, Z. Fu, B. Yu, and J. Wang, ‘‘General construction for XOR-based visual cryptography and its extended capability,’’ Multimedia Tools Appl., vol. 75, no. 21, pp. 13883–13911, Jan. 2016.

[10] Y.-C. Chen, ``Fully incrementing visual cryptography from a succinct non monotonic structure," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1082_1091, May 2017.

[11] Y.-C. Hou and Z.-Y.Quan, ``Progressive visual cryptography with unexpanded shares," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1760_1764, Nov. 2012.

[12] F. Liu and C. Wu, ``Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307_322, Jul. 2011.

[13] D. Wang, F. Yi, and X. Li, ``On general construction for extended visual cryptography schemes," *Pattern Recognit.*, vol. 42, no. 11, pp. 3071_3082, Nov. 2009.

[14] I. Kang, G. R. Arce, and H.-K. Lee, ``Color extended visual cryptography using error diffusion," *IEEE Trans. Image Process.*, vol. 20, no. 1, pp. 132_145, Jan. 2011.

[15] X. Yan, S. Wang, X. Niu, and C.-N. Yang, ``Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality," *Digit.Signal Process.*, vol. 38, pp. 53_65, Mar. 2015.