The Mobile payment based on public-key security technology

Aditya Shah (202003045)

Dhirubhai Ambani Institute of Information & Communication Technology,
Gandhinagar, Gujarat 382007, India
SC 402, Introduction to Cryptography

This article focuses mostly on data security technologies used in China's mobile payment applications. This study will present the commonly used public-key encryption technology and the mobile payment system mode utilised in Chinese mobile payment applications. Reason to do this is that Mobile payment has become a crucial component of e-commerce due to its greater convenience and lower cost. And hence we have to ensure the security of information when making payments.

I. INTRODUCTION

The act of transferring anything of value from one person to another in exchange for the provision of commodities, services, or both is known as payment.The earliest type of payment, however, in which goods or services can be traded between parties, is barter. Cheque, debit, credit, and bank transfers are frequently used forms of payment in the modern world. Payments can be made in the form of stock or other more intricate arrangements in complicated corporate transactions. Exchange of payment is described as the changing of currency, money, and banknotes in terms of the price. While provisioning payment, which is used to transfer money from one account to another, is referred to as the other type of payment.

Electronic payment also refers to mobile payment. It is described as mobile wallet, mobile money, and mobile money transfer. Mobile payment has established itself as a crucial component of e-commerce due to its high convenience and low cost and that is the reason why Mobile payments are becoming a popular replacement for traditional payment methods like cash, checks, and credit cards in today's marketplace. Since the customer can easily pay for a variety of services and goods using his or her standard mobile phone. Since 2008, the use of mobile payments has increased significantly. Therefore, it is crucial to ensure information security while the payment is being processed.

This sort of payment is based on public-key security technology, which is quickly becoming the norm for all transactions. The user's information is safeguarded and transactions are made in a secure manner thanks to this technology. The foundation of public-key security is the idea of encryption. The result of this would be only the receiver which was supposed to receive the message can decode the data that has been exchanged between two parties. This ensures that the data is private and safe from unauthorized access.

In our research A broad theoretical investigation of the structure and method of functioning of the Mobile Payment System (MPS) is carried out. Then we will study of the MPS security mechanism, which takes into account authentication techniques, symmetric and asymmetric encryption, and encryption technologies. Following these, we'll get to the main focus of this study, which is the encryption and decryption of mobile payment transactions using QR codes. Following that, we'll look at the mathematics involved, and after that, we'll take a look at the website our team tried to create in order to better understand the subject.

II. SYSTEM MODEL

A. Functioning Modes

Here we have considered three main functional modes:

1. Mobile operators
2. Banks
3. Third-party service provider

1. Mobile operators

- When mobile operators act as the main body, It uses the mobile number as an account, and the department deducts the mobile payment transaction fees from the user's prepaid account.
- No involvement from the bank is required, and it is difficult to bill the company that does not call.

†Electronic address: 202003045@daiict.ac.in

2. Banks

- When the bank acts as the main body, It connects the bank account to the mobile account by connecting to the mobile network via a dedicated line.
- While mobile operators are not involved in the payment process, banks provide users with business platforms and payment channels.
- The disadvantage of this method is that mobile payment services cannot be networked between banks; Instead, each bank can only provide services to its own bank's users.

3. Third-party service provider

- When a third-party service provider acts as the main body, it is a bridge(connection) between a retailer, a bank, and a wireless service provider.
- Due to user access to multiple third-party bank accounts, third-party providers now play a role in merging users and banks

Let us look at the flow chart of mobile payment process (II A).

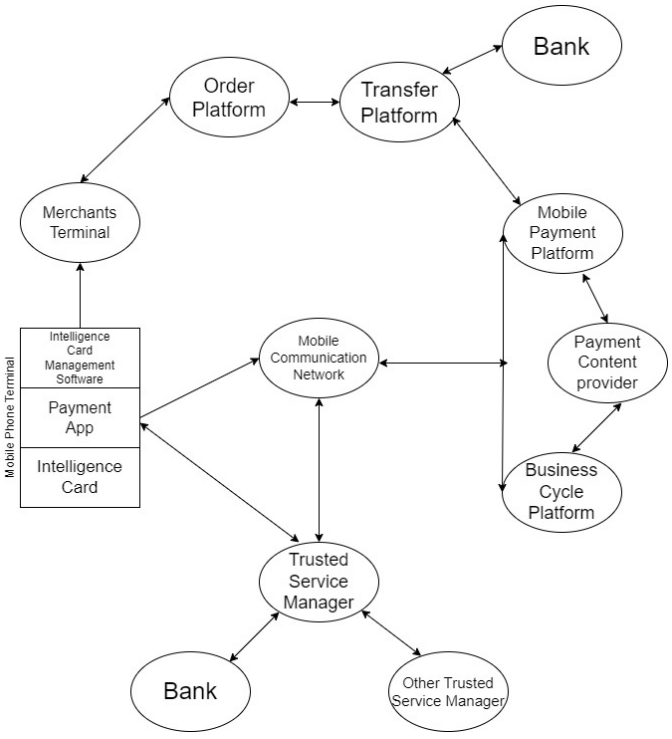

FIG. 1: Flow diagram for Mobile Payment Process

III. SYSTEM STRUCTURE

Mobile Payment System (MPS) is divided into two components:

1. Mobile Payment Agent (MPA)
2. Mobile Payment Platform (MPP)

Here MPA and MPP are connected via digital data network

A. Mobile Payment Agent

Mobile Payment Agent (MPA) is responsible for administration, accounting, and communication at the national level. This is linked to the business operation support system (BOSS).

B. Mobile Payment Platform

Mobile Payment Platform (MPP) is responsible for administration, accounting, and communication at the local level. This is linked to the service providers.

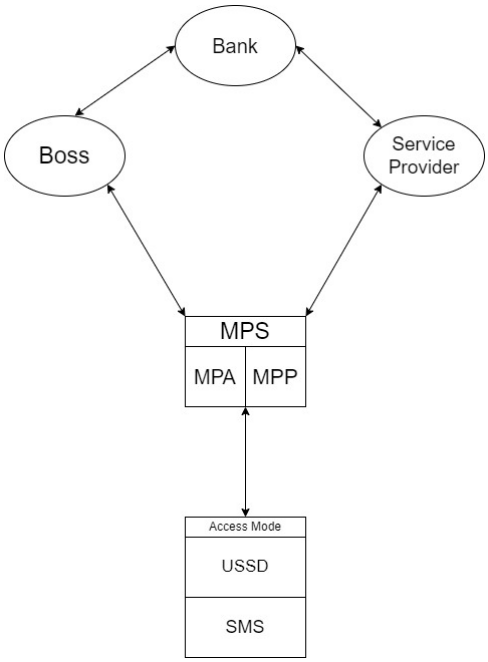

FIG. 2: Flow diagram for system structure

IV. SECURITY MECHANISM

Here, we'll look at the encryption techniques, authenticate these methods, and consider how to guard against

security risks to these encrypted networks while they are accessible to everyone.

A. Encryption Methods

Here we will closely look at two encryption algorithms, Symmetric and Asymmetric Encryption Algorithm.

B. Symmetric encryption

Symmetric encryption uses the same key to encrypt and decode data. This implies that in order to access the encrypted data, both the message's sender and recipient must have the key. Other terms for symmetric encryption include Shared secret encryption and Private-Key encryption. In symmetric encryption, the plain text is converted to cipher text by means of an encryption method, and subsequently converted back to plain text by use of a decryption technique. The plain text is encrypted using the encryption key, and the cipher text is decrypted using the decryption key.

Examples of Symmetric encryption : AES (Advanced Encryption Standard), DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish

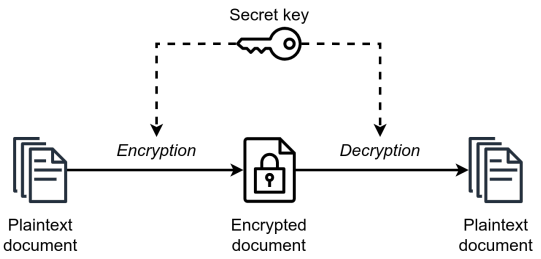

FIG. 3: Following image gives the idea of symmetric key cryptography

C. Asymmetric encryption

Asymmetric encryption, commonly referred to as public key encryption, encrypts and decrypts data using a set of two keys. Whoever desires to send an encrypted message to the key owner can use one key, known as the public key, without paying a fee. The private key, which is used to decode communications encrypted with the public key, is the other key and is kept a secret by the key's owner. Asymmetric encryption uses the recipient's public key to encrypt the data before sending it, and the recipient's private key to decode it after receiving it. Asymmetric encryption provides a better level of security since the private key is never shared or sent.

One of the most used asymmetric encryption techniques is RSA. It employs a key pair made up of a public key and a private key.Numerous applications like security of email, digital signatures and online banking, use RSA.

Applications that call for secure data storage and transport frequently utilise asymmetric encryption. Asymmetric encryption has certain disadvantages even if it offers a better level of protection than symmetric encryption. Its slower processing speed and greater resource requirements are one of its drawbacks. To handle the distribution and use of public keys, which may be complicated and challenging to manage in big organisations, it also necessitates the usage of a public key infrastructure.

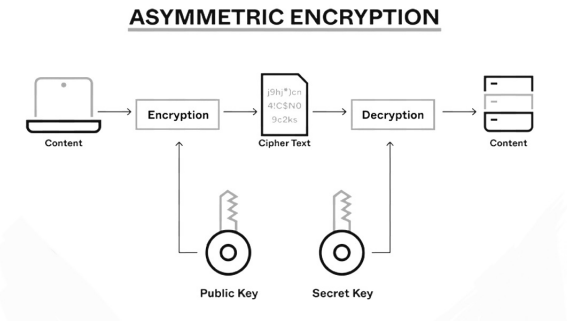

FIG. 4: Following image gives the idea of asymmetric key cryptography(public key encryption)

D. Comparison

Symmetric Cryptosystem ::

For both encryption and decryption, a single key is all that is necessary.
the ciphertext is the same size as the original plain text or smaller.
It takes very little time to encrypt data.
When a lot of data has to be sent, it is utilized.
It is effective because it can handle a lot of data.
Complexity is Low
Security is Low
Examples: AES, DES, ...

FIG. 5:

Asymmetric Cryptosystem ::

A public key and a private key are needed, one for encryption and the other for decryption.
The ciphertext is the same size as the original plain text or bigger.
The encryption method is cumbersome.
It is utilized for modest data transfers.
Due to the limited amount of data it can handle, it is relatively less efficient.
Complexity is High
Security is High
Examples: DSA, RSA, ...

FIG. 6:

V. APPLICATION OF PUBLIC-KEY CRYPTOSYSTEM IN QR CODES

A. What is Barcode ?

FIG. 7: Barcode

A barcode is a visually appealing, machine-readable representation of data. A collection of parallel lines with varied lengths and gaps between them make up a barcode. Some types of barcode is UPC, EAN, Code 39 and QR codes etc... In order to automate the checkout process in food stores, barcodes were originally introduced in the 1940s. Barcodes made it possible to scan product information more quickly and precisely, speeding up the transaction process. Today, barcodes are used in a variety of industries for logistics, inventory control, and product tracking. Additionally, they are utilised in marketing and advertising to give customers more details about the goods or services.

B. Introduction and History of QR Codes

What is a QR code ? is the most fundamental and first question that comes to mind, So let us start with that only. Quick Response (QR) Codes are two-dimensional barcodes that may be read by a QR code reader or a smartphone camera. Denso Wave, a Toyota company, invented QR codes in 1994 with the intention of using them in the automobile sector to monitor manufactured cars.

FIG. 8: QR codes

In a number of contexts, including marketing, advertising, and information exchange, QR codes are employed. For instance, a business may print a QR code

on a product label that links to a website with further details about the item. In order to enter an event, consumers can scan a QR code on their smartphone, which is another way that QR codes are utilised in ticketing.

A multitude of tools and websites may be used to easily produce QR codes. Additionally, many smartphones have built-in QR code scanners, which makes it simple for users to scan codes while on the go.

The possibility that malware or other harmful information may be sent through QR codes is one possible drawback. Users should use caution while scanning codes from untrusted sources and should only do so.

When data is translated into a digital format, QR codes are susceptible to errors, just like other physical methods of storing data. When mistakes happen, Reed-Solomon codes offer a safeguard that permits information to be reliably processed by QR code readers. Finite field arithmetic is used to communicate data in the form of polynomial coefficients. Reed-Solomon codes make it possible to insert logos and insignia into QR codes to promote their function. In this essay, we'll explain how QR codes are created and how error-correcting Reed-Solomon codes are inserted into them. The usage of technologies utilising Maplets will help to demonstrate this.

In conclusion, QR codes offer a flexible and practical approach to distribute information in a variety of contexts. They are a preferred tool for marketers, advertisers, and other businesses due to their capacity to store vast quantities of data and ease of use.

C. Development of QR Codes from traditional Barcodes

Black and white squares are placed in a square grid on a white backdrop to form QR codes. Information such as a website URL, text, or other data is encoded by the squares. The data can be presented on the user's device after a QR code has been scanned and decoded.

The QR code was first only utilised in the automobile sector, but it swiftly spread to other sectors. In the early 2000s, QR codes were being utilised for marketing, advertising, and other purposes. Because users could quickly scan QR codes with their phone's camera after smartphones became widely used in the 2010s, they became even more popular.

The demand for a more adaptable and durable code that could hold more data led to the development of QR codes from standard barcodes. Because they use a 2D matrix format, QR codes can store a lot more data than conventional barcodes. Unlike standard barcodes, which may only hold a few hundred characters, QR codes can hold up to 7,089 characters of data.

D. QR Codes in depth

Different areas of QR Codes are designated for particular purposes. Let us see those ion depth with below figure.

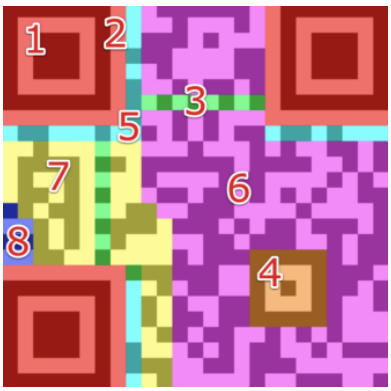

FIG. 9: QR codes

1. *Finder Pattern (1)*

This indicated Position of code.

Three similar structures make up the finder pattern, which can be found in all but the bottom right corner of the QR Code. Based on a 3x3 grid of black modules surrounding by white modules, which are then encircled by black modules, each design is composed of these modules. The decoder programme can identify the QR Code and establish its proper alignment thanks to the Finder Patterns.

2. *Separators (2)*

The white separators, which are one pixel wide and help to distinguish the Finder Patters from the real data, increase their legibility.

3. *Timing Pattern (3)*

This indicated Timing.

The Timing Pattern's black and white modules alternate, allowing the decoder software to calculate each module's width.

4. *Alignment Patterns (4)*

This indicated Alignment of QRCode.

The decoder software uses alignment patterns to help it correct for mild visual distortions. The first generation of QR codes lack alignment patterns. As the code gets bigger, new alignment patterns are added.

5. *Format Information (5)*

This indicated Version Details.

The QR Code's error correction level and the selected masking pattern are both stored in the formation information section, which is composed of 15 bits adjacent to the separators.

6. *Data (6)*

This indicated Data storage.

Data is transformed into a bit stream and then stored in the data section in 8 bit chunks (known as codewords).

7. *Error Correction (7)*

This indicated Error correction zone.

The error correction sector stores error correction codes in 8 bit long codewords, much like the data section does.

8. *Remainder Bits (8)*

This indicated Version Details.

If the data and error-correction bits cannot be separated into 8-bit codewords without leaving a residue, this section is made up of empty bits.

FIG. 10: QR code breakdown

VI. ENCODING OF A QR CODE

QR code uses Reed-Solomon error correction over finite field F_{256} whose elements are encoded as bytes of 8 bits. A QR code mainly stores two types of data: -

- Encrypted data
- Error correction

A. QR Code generation

As discussed in the subsection-QR Codes in depth, a QR Code is made up of several components placed in precise location on a 2-D array.

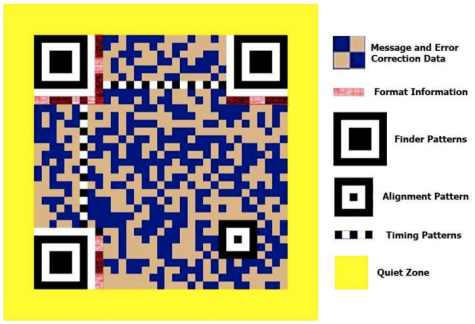

FIG. 11: Summary of QR Code Component

As shown in the figure, the message data and the error correction is stored in the light brown and dark blue squares. Usually bit 1 is represented by dark square and bit 0 by light square. The 'format information' area on a QR Code represents the error correction level and the mask pattern.

The data starts filling in a square from the bottom right corner of the code and follows a zig-zag path (up-down). After the process of data filling is done in the QR code matrix, the process of masking is done so that the QR code is readable by the scanner. In masking, only the data squares are flipped according to their position, i.e. light square becomes light and vice-versa.

B. Error Correction

Error correction is the property of the QR code to restore the encoded data even if the QR code is damaged or dirty. According to the use and the environment, there are 4 error correction levels a user can choose from. The error correction level and their respective code word recovery percentage is mentioned in Table 1.

Error correction level	Recovered code-words (in percentage)
L (Low)	7%
M (Medium)	15%
Q (Quartile)	25%
H (High)	30%

TABLE I: QR code Error Correction Capability

In a QR code, the error correction level is represented by the red line of format information shown in FIG 11. One can easily identify the level of error correction from the following figure.

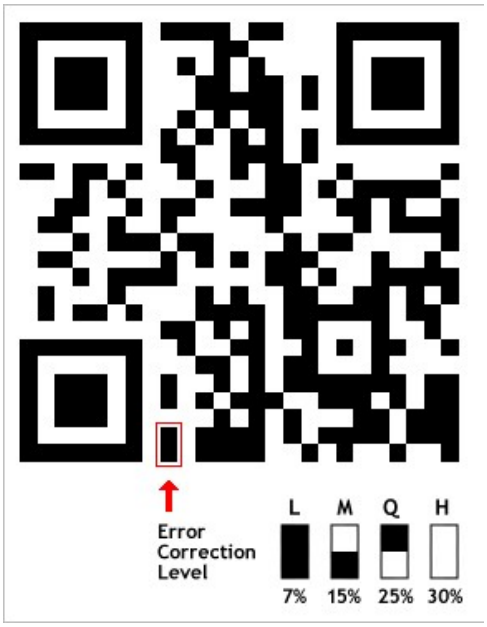

FIG. 12: Error Correction Level on a QR Code

FIG. 13: Different Error Correction Level on a QR Code

Higher error correction capability means that the QR code is able to restore more lost data than a lower error correction capable QR code. So, for higher error correction capability, the error correction zone (shown in fig 9 and fig 10) needs to be large and hence the data storage zone will shrink. This suggests that the quantity of data stored decreases as we increase the error correction level of a QR code.

VII. DECODING OF A QR CODE

The decoding of a QR code is done in the following steps: -

A. Unmasking of a QR code

According to the masking pattern used while encoding in a QR code, the unmasking of a QR code is done with the same mask pattern. After the unmasking is done, the version of the QR code is also identified.

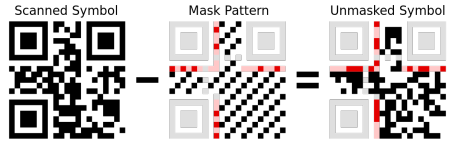

FIG. 14: Unmasking using same mask pattern

B. Indicator and length field

After knowing the version and obtaining the unmasked code, the next step is to find the indicator and the length field.

FIG. 15: Indicator and length field position

The portion of the QR code highlighted in **yellow** is the **indicator**, which is a 4 bits long message used to find encoded message type. The 4 bits which represent different encoded message types are: -

Indicator	Message type
0001	Numeric Encoding
0010	Alphanumeric Encoding
0100	Byte Encoding
0000	End of Message

TABLE II: Message type represented by the indicator

The portion of the QR code highlighted in **blue** is the **length field**. It is a 8 bits long message which is used to find the encoded message length.

C. Final Decoding of message

After unmasking, finding the version of the QR code and obtaining the message type and the message length, the final decoding of the encoded message takes place.

Let us, for example, take a sample QR code: For

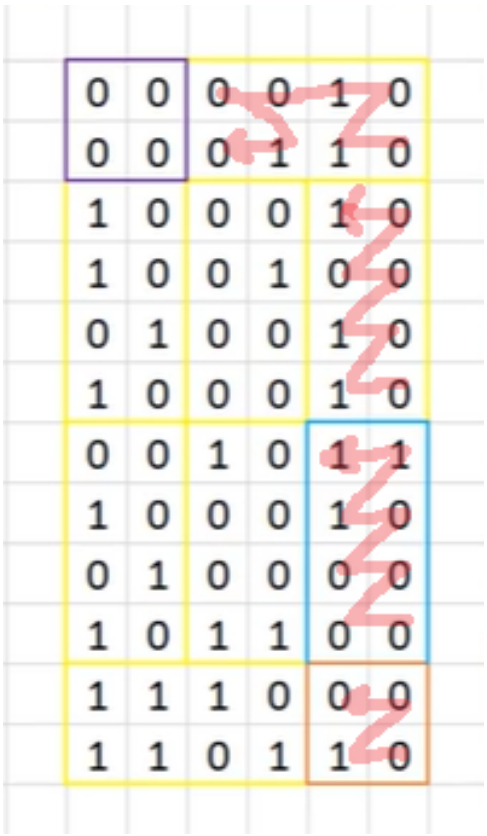

FIG. 16: Sample encoded QR code

decoding, as mentioned earlier, we will start from the bottom right corner of the code and move in a zig-zag pattern (shown in figure). Here, the bits highlighted in

the brown box represents the indicator and will give us the message type. On moving in a zig-zag patter, we obtain the Indicator as 0100 which corresponds to the Byte Encoding (from Table 2).
Now moving further, the bits highlighted in the blue box represents the length field which will give us the message length. Here, the bits are 00000111, which tells us that the length field is 7.
For decoding the encoded message, we move in a similar fashion. On decoding the message, we get the following result: -

Bits	ASCII Value	Character
0101 0001	81	'Q'
0101 0010	82	'R'
0001 0000	32	' '
0100 0011	67	'C'
0110 1111	111	'o'
0110 0100	100	'd'
0110 0101	101	'e'

Hence, we obtain the message as "QR Code".

VIII. SECURITY RISKS OF QR CODE

Even after encoding the data, there are certain risks in the security of a QR code. Some of them are: -

- Malware attack: - Any publicly available QR can be tempered in such a way that anyone who scans the code can get infected by a malware implemented by cyber-criminals in the QR code. The malware can then retrieve the users private information and can even access the camera to get the live feed or even keep a track of the device's location and can also harm the user in several different ways.
- Financial theft: - Considering the rise in the number of contact-less transactions, i.e. through scanning a QR code, it is very easy for a theft actor to replace the legitimate QR code with a fake one such that all transaction money goes into their account.

IX. CONCLUSION

- In this paper, we talked about the mobile payment system based on public-key security technology, different security mechanisms, i.e symmetric and asymmetric encryption. Then we discussed about the application of public-key cryptosystem in QR codes.
- We talked about the History of QR code and the different parts of a QR code. Later we also discussed about the encoding done in the QR code, error correction and then the decoding of a QR code which included unmasking and determining indicator and field length. We also talked about the security risks of a QR code.

X. REFERENCES

- "File: QR Code Masking Example.svg." Wikiversity, https://en.m.wikiversity.org/wiki/File:QRCodeMasking Example.svg.
- The Mathematics of QR Codes - Atcm.mathandtech.org. https://atcm.mathandtech.org/EP2021/invited/21891.pdf
- https://www.google.com/imgres?imgurl
- Sun, Jiabin, and Nan Zhang. "The Mobile payment based on public-key security technology." Journal of Physics: Conference Series. Vol. 1187. No. 5. IOP Publishing, 2019.
- https://blog.qrstuff.com/general/qr-code-error-correction