yesi novaria kunang <yesinovariakunang@binadarma.ac.id>

Reviewer Invitation for EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions

1 message

Journal of Computer Security <em@editorialmanager.com> Tue, Dec 24, 2019 at 3:02 AM
Reply-To: Journal of Computer Security <editorial@iospress.nl>
To: Yesi Novaria Kunang <yesinovariakunang@binadarma.ac.id>

Dear Mrs. Kunang,

You have been invited to review a manuscript for Journal of Computer Security.

I would be grateful if you would review a paper entitled "EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions" for this journal.

This is the abstract:
In recent years, with the rapid development and popularization of e-commerce, the applications of e-coupons have become a market trend. As a typical bar code technique, QR codes can be well adopted in e-coupon-based payment services. However, there are many security threats to QR codes, including the QR code tempering, forgery, privacy information leakage and so on. To address these security problems for real situations, in this paper, we introduce a novel fragment coding-based approach for QR codes using the idea of visual cryptography. Then, we propose a QR code scheme with high security by combining the fragment coding with the commitment technique. Finally, an enhanced QR code-based secure e-coupon transaction framework is presented, which has a triple-verification feature and supports both online and offline scenarios. The following properties are provided: high information confidentiality, difficult to tamper with and forge, and the ability to resist against collusion attacks. Furthermore, the performance evaluation of computing and communication overhead is given to show the efficiency of the proposed framework.

If you would like to review this paper, please click this link: https://www.editorialmanager.com/j-cs/l.asp?i=26488&l=EQU3RC08 *

If you do not wish to review this paper, please click this link: https://www.editorialmanager.com/j-cs/l.asp?i=26489&l=VHQG75RU *

If the above links do not work, please go to https://www.editorialmanager.com/j-cs/ and log on with your user name and password. Your user name is yesikunang. If you do not know your password, you may reset it by clicking this link: https://www.editorialmanager.com/j-cs/l.asp?i=26490&l=4CLEKL2D

The manuscript reference is JCS-191416.

If possible, I would appreciate receiving your review by Jan 22, 2020 (IF JOURNAL IS IN 'INVITATION MODE'). If possible, I would appreciate receiving your review in 30 days (IF JOURNAL IS IN 'AGREED MODE'). You may submit your comments online at the above URL. There you will find spaces for confidential comments to the editor, comments for the author and a report form to be completed.

With kind regards

Javier Lopez
Associate Editor

*If clicking the link above does not open an Editorial Manager window, your email program may have inserted some spaces and/or line markers into the link. Please open a browser window manually and copy and paste the entire link from the email into the url address box. The link starts with the letters "http" and ends with the letters "rev=X" (where X represents a number such as 0,1,2, etc.) Note that the end of the link may be shown on a different line in this email, and may be shown in a different color than the beginning of the link .The entire link must be copied and pasted into the browser in order for the correct Editorial Manager window to be displayed. After copying the link into the url address box, you must also remove any spaces and line markers (e.g. > or >>) by using the delete or backspace keys on your keyboard.

In compliance with data protection regulations, you may request that we remove your personal registration details at any time. (Use the following URL: https://www.editorialmanager.com/j-cs/login.asp?a=r). Please contact the publication office if you have any questions.

yesi novaria kunang <yesinovariakunang@binadarma.ac.id>

Thank you for agreeing to review

1 message

Journal of Computer Security <em@editorialmanager.com> Thu, Jan 2, 2020 at 8:54 AM
Reply-To: Journal of Computer Security <editorial@iospress.nl>
To: Yesi Novaria Kunang <yesinovariakunang@binadarma.ac.id>

Dear Mrs. Kunang,

Thank you for agreeing to review manuscript JCS-191416 for Journal of Computer Security.

I would be grateful if you would review a paper entitled "EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions" for this journal.

To download the paper now, please click this link: https://www.editorialmanager.com/j-cs/l.asp?i=26576&l=FLT6RSEP *

If possible, I would appreciate receiving your review by Jan 22, 2020.

You may submit your comments online at https://www.editorialmanager.com/j-cs/. Your User Name is yesikunang. If you do not know your confidential password, you may reset it by clicking this link: https://www.editorialmanager.com/j-cs/l.asp?i=26577&l=YT36ZP2W

You may also submit your comments using this link: https://www.editorialmanager.com/j-cs/l.asp?i=26578&l=M55I4WF2

There you will find spaces for confidential comments to the editor, comments for the author and a report form to be completed.

With kind regards

Javier Lopez
Associate Editor
Journal of Computer Security

*If clicking the link above does not open an Editorial Manager window, your email program may have inserted some spaces and/or line markers into the link. Please open a browser window manually and copy and paste the entire link from the email into the url address box. The link starts with the letters "http" and ends with the letters "rev=X" (where X represents a number such as 0,1,2, etc.) Note that the end of the link may be shown on a different line in this email, and may be shown in a different color than the beginning of the link. The entire link must be copied and pasted into the browser in order for the correct Editorial Manager window to be displayed. After copying the link into the url address box, you must also remove any spaces and line markers (e.g. > or >>) by using the delete or backspace keys on your keyboard.

Review_Due.ics
1K

yesi novaria kunang <yesinovariakunang@binadarma.ac.id>

Thank you for the review of JCS-191416

1 message

Journal of Computer Security <em@editorialmanager.com> Thu, Jan 16, 2020 at 12:25 PM
Reply-To: Journal of Computer Security <editorial@iospress.nl>
To: Yesi Novaria Kunang <yesinovariakunang@binadarma.ac.id>

Ref.: Ms. No. JCS-191416
EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions
Journal of Computer Security

Dear Mrs. Kunang,

Thank You for your review of this manuscript.

You may access your review comments and the decision letter (when available) by logging on to the Editorial Manager site at

https://www.editorialmanager.com/j-cs/
username: yesikunang
If you do not know your confidential password, you may reset it by clicking this link: https://www.editorialmanager.com/j-cs/l.asp?i=26748&l=NC42IL4N

Kind regards,

Javier Lopez
Associate Editor
Journal of Computer Security

Reviewer Recommendation and Comments for Manuscript Number JCS-191416

EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions

Original Submission
Yesi Novaria Kunang, M.Kom. Reviewer 1

Back | Edit Review | Print | Submit Review to Editorial Office

Recommendation: Accepted pending minor revisions

Overall Manuscript Rating (1 - 100): 75

Custom Review Question(s):	**Response**
Are you willing to review the revision of this manuscript?	Yes
Originality, novelty and significance of results:	Adequate
Technical Quality of Work:	Good
Comprehensibility and Presentation of Paper:	Good
What is the overall impression:	Good

Manuscript Rating Question(s):	**Scale**	**Rating**
Is the article significant to the field?	[1-5]	2
Is the article appropriate for the journal?	[1-5]	3
Is the work an original contribution?	[1-5]	3
Are the conclusions adequately supported by the data?	[1-5]	3
Is the research interesting and important?	[1-5]	3
Is the level of English adequate?	[1-5]	4

Reviewer Comments to Author

There are some changes that should be made to the paper if accepted.
1. Need further investigation to evaluate the security threats performance of the proposed Secure QR codes. The performance evaluations are too limited. The author only evaluate the efficiency side of the running time overhead and delay.
2. In the description of Figure 5, it would be helpful to give detail explanation why at the computing phase of the QR code version has a significant effect on running time overhead.
3. Further Discussion in Figure 6, it would be helpful to explain why the decoding process more efficient.
4. The statements in figures 9 and 10 describe the end to end delay for EQRC-I or EQRC- II or both of them?

Reviewer Confidential Comments to Editor:

There is no a financial or other conflict of interest between my work and that of the authors.

Please give a frank account of the strengths and weaknesses of the article:

Strengths:
The manuscript reported by Liu et al. has some interesting ideas and results on a subject well investigated. Most of the study is well designed, and the scientific value is given enough.

Weaknesses:
Valid work but limited contribution. This Paper has contributions but not significant within its area of research

Back | Edit Review | Print | Submit Review to Editorial Office

Completed Reviewer Assignments for Yesi Novaria Kunang, M.Kom.

Page: 1 of 1 (1 total assignments) Display 10 results per page.

Action	My Reviewer Number	Manuscript Number	Article Type	Article Title	Current Status	Final Disposition	Date Reviewer Invited	Date Reviewer Agreed	Date Review Due	Date Review Submitted	Days Taken	Editor's Name
View Reviewer Comments Send E-mail	1	JCS-191416	Research Article	EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions	Under Review		Dec 23, 2019	Jan 01, 2020	Jan 22, 2020	Jan 16, 2020	24	Javier Lopez

Page: 1 of 1 (1 total assignments) Display 10 results per page.

<< Reviewer Main Menu

You should use the free Adobe Reader 10 or later for best PDF Viewing results.

Journal of Computer Security

EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions

--Manuscript Draft--

Manuscript Number:	JCS-191416
Full Title:	EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions
Article Type:	Research Article
Keywords:	QR code; e-coupon; e-commerce; commitment algorithms; visual cryptography
Abstract:	In recent years, with the rapid development and popularization of e-commerce, the applications of e-coupons have become a market trend. As a typical bar code technique, QR codes can be well adopted in e-coupon-based payment services. However, there are many security threats to QR codes, including the QR code tempering, forgery, privacy information leakage and so on. To address these security problems for real situations, in this paper, we introduce a novel fragment coding-based approach for QR codes using the idea of visual cryptography. Then, we propose a QR code scheme with high security by combining the fragment coding with the commitment technique. Finally, an enhanced QR code-based secure e-coupon transaction framework is presented, which has a triple-verification feature and supports both online and offline scenarios. The following properties are provided: high information confidentiality, difficult to tamper with and forge, and the ability to resist against collusion attacks. Furthermore, the performance evaluation of computing and communication overhead is given to show the efficiency of the proposed framework.

December 6, 2019

Dear JCS Editors and reviewers,

The paper titled “EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions” has been submitted to the Journal of Computer Security. Please accept it as a candidate for publication.

A preliminary version of this work has been presented at the IEEE International Conference on Communications (ICC) 2019. In that paper, three main contributions provided are as follows: first, we proposed a fragment coding-based approach for QR codes with the idea of visual cryptography. Second, an enhanced QR code scheme with a higher security is proposed by combining the fragment coding and commitment technique. Third, we proposed an online secure e-coupon transaction framework with a triple-verification mechanism, based on the techniques above. Comparing with traditional e-coupon schemes, the proposed framework can efficiently resist against the information leakage, eavesdropping, modification, forgery, replay attack, and collusion attack.

Considering the limitations in the published paper, we made further improvements in this paper. There are at least 40% updates and difference, which are mainly listed as follows:

1. An offline secure e-coupon transaction framework is proposed, where customers do not connect to the Internet directly. An audit trail approach is involved to solve disputes. The property of supporting both online and offline scenarios provides a comprehensive protection for the real situations of e-coupon transaction services.
2. We provide stronger security analyses on the digital signature, encryption, commitment, HMAC, QRFC approach, and triple verification. The improved analyses are based on cryptographic assumptions, mathematical properties, and potential attacks.
3. To evaluate the performance further, we conduct a comprehensive simulation to analyze the communication overhead on OMNeT++ 5.5. The effects of the length of messages transmitted and the scale of users are considered on the end-to-end delay. Results show that the transaction framework we proposed has a good efficiency.

Thanks for your time in handling the review process of our paper. Please feel free to contact us if you have any questions or concerns.

Sincerely yours,

Rui Liu, Jun Song, Zhiming Huang, Jianping Pan

EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions [1]

Rui Liu [a], Jun Song [b,*], Zhiming Huang [a] and Jianping Pan [a]
[a] *Department of Computer Science, University or Victoria, Victoria, Canada*
[b] *School of Computer Science, China University of Geosciences, Wuhan, Hubei, China*

Abstract. In recent years, with the rapid development and popularization of e-commerce, the applications of e-coupons have become a market trend. As a typical bar code technique, QR codes can be well adopted in e-coupon-based payment services. However, there are many security threats to QR codes, including the QR code tempering, forgery, privacy information leakage and so on. To address these security problems for real situations, in this paper, we introduce a novel fragment coding-based approach for QR codes using the idea of visual cryptography. Then, we propose a QR code scheme with high security by combining the fragment coding with the commitment technique. Finally, an enhanced QR code-based secure e-coupon transaction framework is presented, which has a triple-verification feature and supports both online and offline scenarios. The following properties are provided: high information confidentiality, difficult to tamper with and forge, and the ability to resist against collusion attacks. Furthermore, the performance evaluation of computing and communication overhead is given to show the efficiency of the proposed framework.

Keywords: QR code, e-coupon, e-commerce, commitment algorithms, visual cryptography

1. Introduction

With the rapid development of electronic payment systems and digital marketing, e-coupons (Electronic Coupons) have become increasingly popular. Because e-coupons are easy to manage, quick to distribute, and eco-friendly, they are widely accepted as a replacement of paper coupons by many companies, such as Shoppers Drug Mart, McDonald's, Air Canada and so on. Besides, the various type of e-coupons, including but not limited to discount coupons, cash coupons, pre-paid cards and rechargeable cards, are appropriate for different uses in the market. The demands for e-coupon services include easy generation, fast readability, large storage capacity, error recovery and so on. QR (Quick Response) codes support the above properties well and thus are universally preferred.

Although QR codes have been widely used in many domains, such as mobile payment, document verification, commodity management, inventory checking, parcel tracking and so on, security incidents still occur frequently and the situation becomes increasingly serious. Economic losses and privacy leak which are caused by scanning malicious QR codes are reported many times. Cadger *et al.* [2] analyzed 12 different software packages which can decode QR codes, and found that none of them has the ability

[1] A preliminary version of this paper appeared in 2019 IEEE International Conference on Communications (ICC) [1]
[*] Corresponding author. E-mail: songjun@cug.edu.cn.

to detect a tampered QR code. Besides, scanning QR codes with sensitive personal information, such as tickets, payment codes and so on, poses a dramatic threat to the privacy of users. The risks above are mainly due to the open coding scheme of QR codes, plaintext format of the content in QR codes, and lack of verification mechanisms. Without proper measures and solutions, QR codes cannot be used in online transactions safely.

The studies on the security of QR codes are increasingly hot in recent years. Many research focuses on the anti-phishing of QR codes with the techniques of link detection, digital signature and so on [3–5]. There is also some work using cryptography and steganography to provide the confidentiality of QR codes [6, 7]. However, due to the specific threats of e-coupon services, *e.g.*, the collusion attack between merchants and customers, tempering or forgery of e-coupons, and liability disputes among users, these research cannot be applied well to the QR code-based e-coupon transaction services.

To address the above concerns, in this paper, we propose an enhanced QR code and triple-verification-based secure e-coupon transaction framework EQRC. It mainly aims at the common security risks such as the plaintext transmission, collusion attack, forgery and tampering in e-coupon services. Using encryption and scrambling, anonymous authentication, and commitment, EQRC has the ability to ensure data confidentiality and provide anti-tampering, anti-forgery, signature verification for both online and offline scenarios. The main work and contributions of this paper include the following four aspects:

(1) We proposed a fragment coding-based approach for QR codes, which is based on the idea of visual cryptography. Due to the pseudo-randomness of fragments, it is hard to guess the true information of the original QR code from one of the split code pair. Thus, the safety of QR codes is enhanced efficiently as the attacker would be more difficult to access the original QR code.
(2) We proposed an enhanced QR code scheme with a higher security, which is inspired by the fragment coding and commitment technique. This scheme not only has the ability to prevent the leakage of sensitive information in QR codes, but also can effectively reduce the security risks caused by QR code tampering or forgery.
(3) We proposed a secure online e-coupon transaction framework EQRC, which relies on the enhanced QR codes with digital signature and commitment. EQRC provides three verifications, i.e., message digest computing, enhanced QR codes stacking and commitment opening. Due to these three verifications, our framework can provide integrity and authenticity for e-coupons.
(4) We extended EQRC from online to offline. In both of the scenarios, users can use e-coupons with the same security and privacy properties provided. The collusion attack between merchants and customers can be resisted effectively. Furthermore, in the offline scenario, liability disputes can be settled with an audit trail.

In addition, we analyzed and proved the security of EQRC based on cryptographic assumptions, mathematical properties, and potential attacks. The comprehensive evaluations of the computation overhead, encoding and decoding overhead, and communication overhead are provided. Results show that the proposed framework has a good performance in security and efficiency.

In the rest of this paper, Section 2 shows the related work, and briefly introduces the system model, security goals and threats. Related cryptographic techniques are also presented. Section 3 gives the detailed description of the schemes proposed in this paper. The security and performance evaluation are presented in Section 4 and 5 respectively. Section 6 concludes the paper and discusses the future work.

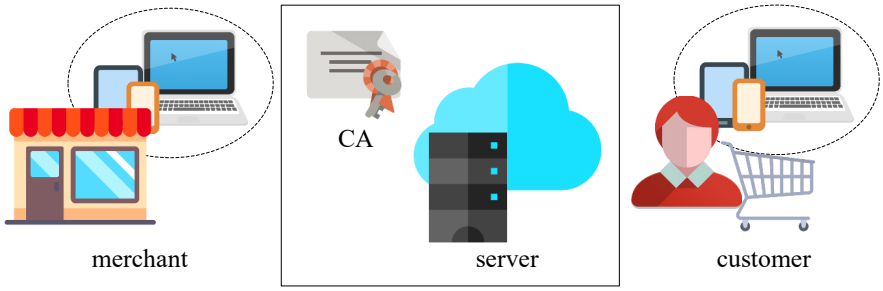

Fig. 1. System model

2. Preliminaries

2.1. Related Work

QR codes are commonly used for holding data. Protecting the content of QR codes is a hot topic in these years. Cheng *et al.* [8] proposed an innovative secret sharing scheme for QR code applications. The proposed scheme uses the XVCS (XOR-based Visual Cryptography Scheme) theory and has more flexible access structures. Lin *et al.* [9] proposed a secret hiding mechanism based on QR code error correction with a high capacity. Tkachenko *et al.* [10] proposed a two-layer QR code-based scheme for sharing secret messages, which replaces the black blocks in the traditional QR code with a specific pattern. Although these strategies can effectively protect the contents of QR codes to some extent, they cannot be adopted well in e-coupon transactions where both malicious merchants and customers should be considered.

To solve the problem of forgery and tampering, some effective techniques are presented. Zhang *et al.* [11] proposed a message authentication scheme with the help of roadside units for vehicular communications. The scheme has a better performance than previous work in message loss ratio and delay. Considering the large amount of information generated in vehicular networks at the same time, Lee and Lai [12] presented a secure batch verification scheme based on bilinear pairing. Hasan *et al.* [13] designed a secret information verification mechanism based on an authentication chain. Although this mechanism has the characteristic of traceability and anti-counterfeiting, it is not suitable for QR code services as keeping a chain for each QR code is space-consuming.

As for the anonymous digital signature technique which is often adopted for authentication, many related studies have been reported. Brickell *et al.* [14] proposed the direct anonymous attestation (DAA) in 2004. Based on zero-knowledge proof and the idea of group signature, users in DAA can obtain identity-anonymous certificates without revealing privacy information. Chen *et al.* [15, 16] proposed a pairing-based DAA protocol in the asymmetric setting in 2009 and proposed a threshold anonymous authentication (TAA) scheme for vehicular ad-hoc network (VANET) in 2011, which is adopted in our paper for e-coupon services.

2.2. System Model

We consider a system model comprised of four entities, which are shown in Figure 1:

(1) Root certificate authority (CA): a root certificate authority generates and distributes keys for other entities. It issues certificates to merchants and customers. CA is trusted by other entities in the model.

(2) Merchant: a merchant provides services or goods to customers. It can support e-coupon transactions but may be a malicious entity.
(3) Customer: a customer uses e-coupons when buying services or goods from a merchant. It also may be a malicious entity and may be in collusion with a merchant.
(4) Server: a trusted server manages transactions with e-coupons. The main functions include e-coupon generation, e-coupon distribution, authentication, verification, e-coupon updating and so on. Besides, it handles disputes when necessary.

The scenarios of online transactions and offline transactions are considered in this work. In both scenarios, the server generates the e-coupons, i.e., enhanced QR code pairs, and distributes them to the merchant and customer, respectively.

(1) Online transactions allow the customer to finish transactions remotely on computers or mobile phones. Both the customer and the merchant need to send one enhanced QR code to the server, respectively. Note that the merchant only sends it when receiving the request from the server, which means there is no direct interaction between the merchant and the customer. The server will process the verification and payment when receiving the QR codes.
(2) In offline transactions, the customer does not directly connect to the server, but send the encrypted and signed QR code to the merchant through near-field communications, e.g., bluetooth technologies. The merchant then sends his own QR code with the customer's one to the server. As there is a direct interaction between merchants and customers, disputes need to be resolved.

2.3. Security Goals and Threats

In this paper, we aim at achieving the following security goals,

(1) *Authentication*: merchants and customers must be authorized by a CA. In a transaction, the identities of both the merchant and the customer should be verified;
(2) *Data integrity*: no adversary can temper or damage e-coupons without being detected;
(3) *Data authenticity*: the server with EQRC should be able to detect the e-coupons forged by adversaries;
(4) *Data confidentiality*: the sensitive data of e-coupons is only visible to the server. Any other entities including merchants and customers cannot get the access;
(5) *Identity anonymity*: the true identity of a user should not be exposed during signing and verification so that the user privacy is preserved.

Besides, the integrity and authentication of the messages sent between entities should also be guaranteed.

The threats in e-coupon transaction services we focus on are *information leakage*, *message eavesdropping*, *message modification*, *message forgery*, *message replay attack* and *collusion attack* between a merchant and a customer. *Liability disputes* are also considered.

2.4. Cryptographic Techniques

In this section, we briefly introduce the cryptographic tools adopted in our framework.

(1) *Group Signature*: Group signature allows a user of a group to sign a message anonymously. With a group signature scheme, a signature σ to a message m can be generated by $\mathtt{Sig}_{(sk,pk)}(m)$ where

sk is the secret key of the signer and *pk* is the public key of the group. σ can be verified by $\texttt{Ver}_{pk}(\sigma, m)$. Given a message m and its signature σ, it is not feasible to find out the identity of the individual signer without the secret key of the revocation manager. Besides, only a member in the group can generate a valid signature. With these properties, group signature can be well used in anonymous authentication.

In this paper, we adopt an effective group signature-based authentication scheme TAA [16] and adapt it to e-coupon services. It allows every legitimate user to obtain credentials by algorithms $Setup$ and $Join$, and provides anonymous signatures and message verification by algorithms $Sign$ and $Verify$.

(2) *Commitment*: Commitment is a basic cryptographic tool which allows one to keep the sensitive information hidden to others while maintaining the ability to reveal it. It usually comprises a generation phase, a commitment phase and an opening phase. In the generation phase, given generators g, h and a security parameter k, a key generation algorithm `Gnrt` outputs public parameters for the commitment scheme. Note that `Gnrt` is normally run by a trusted third party. In the commitment phase, the commitment *com* to a value m is computed with a parameter *open* as $com = \texttt{Comm}(m, open)$. The opening phase is also named as reveal phase, in which m is revealed and checked with $\texttt{Opnv}(com, m, open)$. The entities in a commitment scheme are a sender and a receiver.

The Pedersen commitment scheme [17] is adopted in our work. It is based on the **Discrete Logarithm Problem** (DLP). In Pedersen commitment, *open* is set as $r \in \mathbb{Z}_q$. The commitment to a value $m \in \mathbb{Z}_q$ can be defined as $com = \texttt{Comm}(m, r) = g^m h^r$ where g and h are elements of $\mathbb{G}_q$ such that only the receiver knows $\log_g h$. Then the receiver can check if $\texttt{Opnv}(com, m, r) = true$ by recomputation when m and r are both revealed. The Pedersen commitment scheme is a perfect-hiding scheme, binding under the discrete logarithm assumption.

(3) *Visual Cryptography*: Visual cryptography allows visual information such as pictures to be encrypted in such a way that the decryption can be performed by human vision instead of algorithms [18]. One well-known secret sharing scheme based on visual cryptography [19] is achieved by breaking up an image `fig` into n shares, say $\mathscr{A} = \{\texttt{fig}_0, \texttt{fig}_1, \ldots, \texttt{fig}_{n-1}\}$. The original image can be decrypted by overlaying all the elements in $\mathscr{A}$. Any proper subset $\mathscr{B}$ in $\mathscr{A}$, i.e., $\mathscr{B} \in \mathscr{A}$ but $\mathscr{B} \neq \mathscr{A}$, cannot reveal information about `fig`.

With the idea of visual cryptography, we proposed a fragment coding-based approach for QR codes. Each QR code can be easily split into two parts and recovered quickly, while it is hard for an adversary to get the original code by any one of the parts. The approach is described in detail in Section 3.2.

(4) *One-way Function and Randomness*: One-way function is a wide-used cryptography tool, which is easy to check but hard to invert. To be specific, for any randomized algorithm $\mathcal{F}$ which attempts to compute a pseudo-inverse for a one-way function f, any positive integer c and sufficiently large n, we have [20]:

$$\Pr[f(\mathcal{F}(f(x))) = f(x)] < \frac{1}{n^c}. \tag{1}$$

One particular application of one-way function is the keyed-hash message authentication code (HMAC). HMAC is usually used for message authentication and integrity.

In the design of the enhanced QR codes, we adopted SHA-2 (Secure Hash Algorithm 2) as the hash function used in the HMAC. SHA-2 is an iterated hash function, using the Merkle-Damgård structure. The Merkle-Damgård structure defines a hash function h based on an external one-way

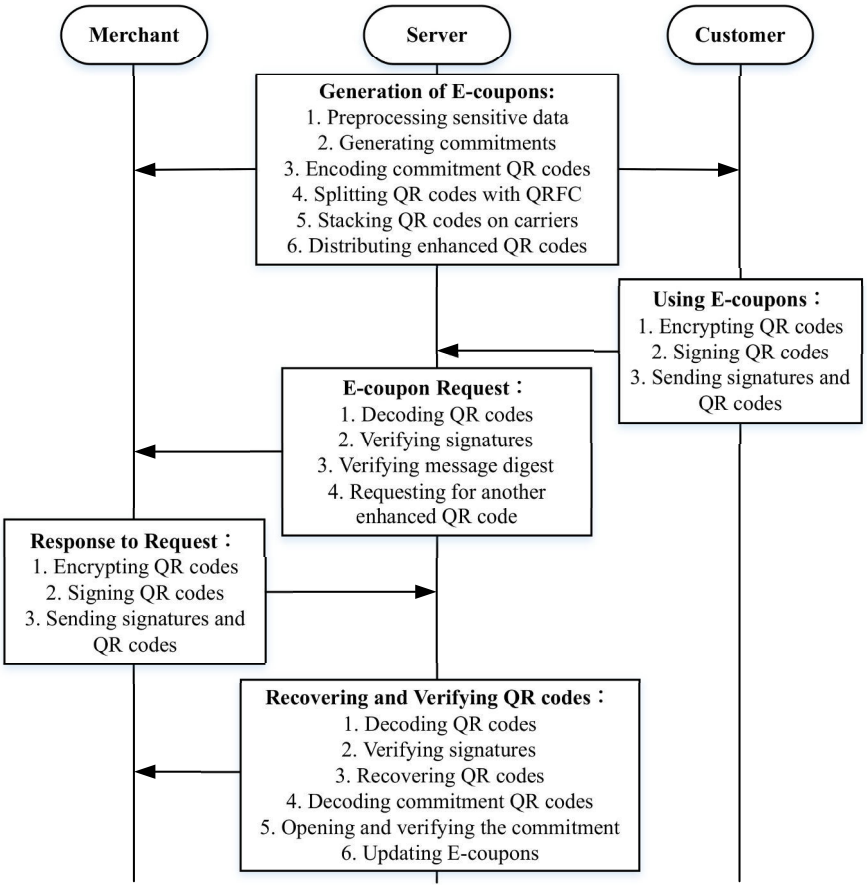

Fig. 2. Protocol flow of EQRC-I

compression function $f : \{0,1\}^{m+n} \to \{0,1\}^m$ where $n \geqslant 2$. With HMAC-SHA-2, the modification and forgery attack can be resisted.

Additionally, one-way function can also apply to Pseudorandom Number Generators (PRNGs) in this work. A PRNG is a deterministic polynomial-time algorithm $\mathcal{G} : \{0,1\}^n \to \{0,1\}^{l(n)}$ mapping a uniformly chosen short string called seed to a longer string where l is a stretching function. The output $\mathcal{G}_n$ is computational indistinguishable from a uniform distribution $\mathcal{R}_n$ on $\{0,1\}^{l(n)}$ where $n \in \mathbb{N}$ [21]. With a PRNG, the output of the fragment coding-based approach we proposed is pseudo-random. The confidentiality, authenticity and integrity are ensured with this property. The details are given in Section 4.5.

3. Framework Design

In this section, we first provide the details of the framework design of EQRC-I, which is used for online scenarios. Then we briefly talk about the framework of EQRC-II for offline scenarios. The protocol flow of EQRC-I is shown in Fig. 2. There are five main algorithms, namely Enhanced QR Coding (Alg. 1), Signing (Alg. 2), Verification (Alg. 3) and Recovery (Alg. 4).

The notations of our framework are listed in Table 1.

Table 1
Notations

Notation	Descriptions
S	A server
M	A merchant
C	A customer
$isk(x, y)$	The dualistic secret key of CA
(pk, sk)	A key pair: (public key, secret key)
key	A secret key of M, managed by S
$data_0$	The sensitive data of an e-coupon
$data$	The data of $data_0$ after preprocessing
msg	The message needs to be sent or received
com	A commitment result
$\overline{QR}$	The standard QR code of com
$(\overline{QR^1}, \overline{QR^2})$	A pair of patterns generated from $\overline{QR}$
$\overline{CQR}$	A carrier QR code
$(\overline{SQR^1}, \overline{SQR^2})$	A pair of enhanced QR codes
$\overline{ESQR}$	A QR code generated by $(\overline{SQR^1}, \overline{SQR^2})$

3.1. Protocol Setup

There is a trusted certificate authority CA in the framework we proposed. CA distributes key pairs (pk_S, sk_S), (pk_M, sk_M) and (pk_C, sk_C) for trusted servers S, merchants M and customers C, respectively. Besides, CA generates a secret key key for each M, which is secret to M and hosted in S.

In addition, for message signature, CA issues triplet certificates for users, i.e., merchants and customers, which provides the authentication of users. The protocol setup is similar to that in [16] and [22]. Three cyclic groups $\mathbb{G}_1 = \langle P_1 \rangle$, $\mathbb{G}_2 = \langle P_2 \rangle$ and $\mathbb{G}_T$ of sufficiently large prime order q are chosen. P_1 and P_2 are two random generators. A pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is chosen with following properties:

(1) *Bilinear*: $\hat{e}(aP_1, bP_2) = \hat{e}(P_1, P_2)^{ab}$ holds for any two integers $a, b \in \mathbb{Z}_q$;
(2) *Non-degenerate*: $\hat{e}(P_1, P_2) \neq 1_{\mathbb{G}_T}$ where $1_{\mathbb{G}_T}$ is the identity element of $\mathbb{G}_T$;
(3) *Computable*: there exists a polynomial time algorithm for computing $\hat{e}(P, Q)$ for $\forall P \in \mathbb{G}_1$ and $\forall Q \in \mathbb{G}_2$.

The triple certificates (A, B, C) are constructed with users' true identities f and the secret key of CA, i.e., the bigram $isk(x, y)$. To be specific, $A \leftarrow r \cdot P_1$, $B \leftarrow y \cdot A$ and $C \leftarrow (x \cdot A + fxy \cdot A)$ where r is a random integer in $\mathbb{Z}_q$. Then each certificate can be used to sign messages for a specific user. More details are in [16].

3.2. Generation of Enhanced QR Codes

The framework we proposed is based on an enhanced QR code scheme. With this scheme, a standard QR code is processed to finally generate a pair of enhanced QR codes $(\overline{SQR^1}, \overline{SQR^2})$, which can be seen as two fragments of an e-coupon. Enhanced QR codes ensure the confidentiality of e-coupons and are hard to tamper with or forge.

Algorithm 1 Enhanced QR Coding

procedure ENCODING(Sensitive Data $data$)
  $(com, decom) \leftarrow Com(crs, data)$
  $\overline{QR} \leftarrow Encode(com)$
  $(\overline{QR^1}, \overline{QR^2}) \leftarrow Split(\overline{QR})$
  $\overline{SQR^1} \leftarrow Stack(\overline{QR^1}, \overline{CQR})$
  $\overline{SQR^2} \leftarrow Stack(\overline{QR^2}, \overline{CQR})$
return $(\overline{SQR^1}, \overline{SQR^2})$
end procedure

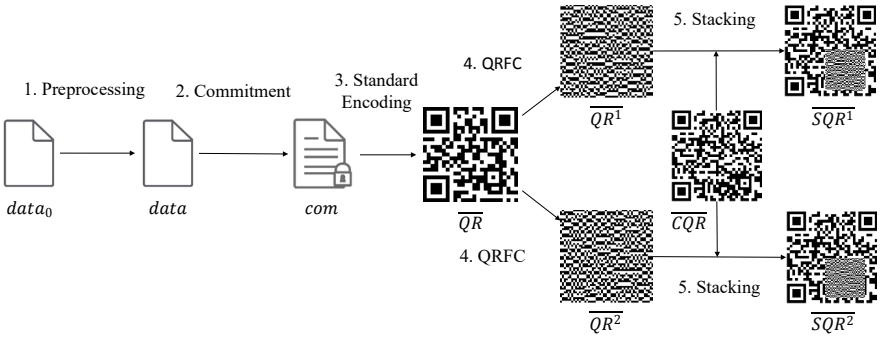

Fig. 3. Generation of enhanced QR codes

The generation flow of enhanced QR codes is shown in Fig. 3. As Algorithm 1 discusses, there are four main functions in the generation process: 1) $Com(crs, data)$ denotes the commitment process on the sensitive data $data$ with the parameter crs. It returns a commitment com and a parameter $decom$ to open the commitment. 2) $Encode(com)$ returns a standard QR code with the specific content com. 3) $Split(\overline{QR})$ returns a pair of pseudo-random patterns with a fragment coding-based approach on a standard QR code $\overline{QR}$. 4) $Stack(\overline{QR^1}, \overline{CQR})$ is a graphic combination between an enhanced QR code $\overline{QR^1}$ and a carrier QR code $\overline{CQR}$. Some details are given as follows.

3.2.1. Commitment

Consider the capacity of QR codes and the size of commitments, the sensitive data $data_0$ in an e-coupon can be first preprocessed to $data$ through a hash function, as the first step shown in Fig. 3. To ensure the confidentiality of $data_0$, as Step. 2, we use the Pedersen commitment technique to generate the commitment $com = g^{data}h^r \mod p$ where (p, g, h, r) are security paratmeters [17]. With such a perfect-hiding commitment scheme, even though M and C conduct the collusion attack, they can get nothing of $data_0$ from com.

3.2.2. QRFC Approach

With the idea of visual cryptography, we introduce QRFC, a fragment coding-based approach for QR codes. Through QRFC, we can split $\overline{QR}$, i.e., a standard QR code encoded with com by Step 3, to two fragments $(\overline{QR^1}, \overline{QR^2})$. The details are as follows. We use k bits 0 and 1 to denote the black and white blocks in an original QR code $\overline{QR}$, i.e., $\{0,1\}^k$, where $k \in \{k = 2k_0 | k_0 \in \mathbb{N}^* \wedge k_0 > 0\}$. Thus, one block has 2^k types of code words, i.e., $Str = \{r_0 r_1 \cdots r_{k-1} | r_i = 0 \vee 1, 0 \leqslant i \leqslant k-1\}$.

Define $S^0 = \{r_0 r_1 \cdots r_{k-1} | r_0 = 0\}$, $S^1 = \{r_0 r_1 \cdots r_{k-1} | r_0 = 1\}$. If a block in $\overline{QR}$ is black, the corresponding code words, i.e., Str^1 in $\overline{QR^1}$ and Str^2 in $\overline{QR^2}$, should satisfy $Str^1 + Str^2 (\mathsf{mod}\ 2) = S^0$. If the block is white, $Str^1 + Str^2 (\mathsf{mod}\ 2) = S^1$.

With the rule above, all blocks in $\overline{QR}$ are re-encoded randomly to two sequences. Turn each 0 in sequences to a black pixel and 1 to a white pixel so that $\overline{QR^1}$ and $\overline{QR^2}$ are finally generated.

We choose $k = 4$ in our framework. The construction method is shown in Table 2. The choice from *Choice* for any block is pseudo-random with the help of PRNGs, which does not affect the success of decoding.

Table 2
QRFC Approach ($k = 4$)

Block in $\overline{QR}$	Choice	$\overline{QR^1}$	$\overline{QR^2}$
black	1	1001	1001
	2	0110	0110
white	1	1001	0110
	2	0110	1001

3.2.3. Carrier QR Codes

As customers need an easy way to access some public information, such as the merchant's name, the expiry date of the coupon and the discount amount, we introduce a standard QR code, say carrier QR code $\overline{CQR}$. $\overline{CQR}$ also maintains a hash of $\overline{QR^1}$, $h(\overline{QR^1})$, which can be used to verify $\overline{QR^1}$. $h(\overline{QR^1})$ is generated through HMAC-SHA2 with the corresponding secret key *key*. The security provided by $h(\overline{QR^1})$ is analyzed in detail in Section 4.5.

Based on the *Reed-Solomon* error correction code used in QR codes, the enhanced QR codes $\overline{SQR^1}$ and $\overline{SQR^2}$ can be generated by Step 5, i.e., embedding $\overline{QR^1}$ and $\overline{QR^2}$ into $\overline{CQR}$ separately without damaging the necessary data in $\overline{CQR}$. Note that $\overline{SQR^1}$ and $\overline{SQR^2}$ use the same $\overline{CQR}$ and the same embedding position for future processing. More explanation is given in Section 3.4.

Note that S distributes $\overline{SQR^1}$ to C and $\overline{SQR^2}$ to M after the generation.

3.3. Signing and Verification

To protect the messages sent between entities, we introduce encryption and anonymous authentication techniques. In this section, we mainly talk about the transaction process instead of the distribution process of S. Before being sent, a message must be encrypted and signed. $(\overline{SQR})_{pk_S}$ denotes the ciphertext of $\overline{QR^1}$ or $\overline{QR^2}$ using *ElGamal* algorithm with pk_S. The anonymous authentication scheme we introduce is similar to [16] and [22].

Algorithm 2 performs the signing on message msg and generates a signature σ by an entity U. In this algorithm, (R, S, T) can be seen as an anonymous certificate. c and s provide the correlation proof of (R, S, T) and the true identity of the entity U. n_t is a timestamp to defend against the replay attack. $\hat{e}$ is a map function [16] from $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. H is a hash function $\{0,1\}^* \to \mathbb{Z}_q$.

The verification algorithm carried out by S is shown in Algorithm 3. $Dec_{sk_S}(msg)$ is a decryption function of msg under sk_S. Because $S = a \cdot B = ay \cdot A = y \cdot R$, $\hat{e}(R, Y) = \hat{e}(A, P_2)^{ay} = \hat{e}(S, P_2)$ can be checked first. Then S re-computes τ from the elements it holds and checks the consistency of c.

Algorithm 2 Signing

procedure SIGNING(Message msg)
  if $U = C$ **then** $msg \leftarrow \overline{SQR^1}$
  else if $U = M$ **then** $msg \leftarrow \overline{SQR^2}$
  end if
  $a \leftarrow \mathbb{Z}_q;\ z \leftarrow \mathbb{Z}_q; R \leftarrow a \cdot A;\ S \leftarrow a \cdot B;\ T \leftarrow a \cdot C;$
  $\tau \leftarrow \hat{e}(S,X)^z; c \leftarrow H(R||S||T||\tau||n_t||msg)$
  if $U = C$ **then** $s \leftarrow z + c \cdot sk_C \pmod q$
  else if $U = M$ **then** $s \leftarrow z + c \cdot sk_M \pmod q$
  end if
  $\sigma \leftarrow (R,S,T,c,s,n_t)$
return σ
end procedure

Algorithm 3 Verification

procedure VERIFICATION(Message msg, Signature σ)
  $msg = (\overline{SQR})_{pk_S}$
  $demsg \leftarrow Dec_{sk_S}(msg)$
  if $\hat{e}(R,Y) \neq \hat{e}(S,P_2)$ **then**
    return Reject
  end if
  $\rho_a^\dagger \leftarrow \hat{e}(R,X); \rho_b^\dagger \leftarrow \hat{e}(S,X); \rho_c^\dagger \leftarrow \hat{e}(T,P_2)$
  $\tau^\dagger \leftarrow (\rho_b^\dagger)^s \cdot (\rho_c^\dagger/\rho_a^\dagger)^{-c}$
  if $c \neq H(R||S||T||\tau^\dagger||n_t||demsg)$ **then**
    return Reject
  end if
return Accept
end procedure

3.4. Recovery and Triple Verification

Once receiving a pair of enhanced QR codes $\overline{SQR^1}$ and $\overline{SQR^2}$, S is able to recover and verify e-coupons. Algorithm 4 describes the details of the recovery. It contains three main processes: 1) the decoding process of QRFC. Because the carrier QR codes of $\overline{SQR^1}$ and $\overline{SQR^2}$ are the same, with computing $\overline{SQR^1} + \overline{SQR^2} \pmod 2$, $\overline{CQR}$ turns to be all 0. Thus, $\overline{ESQR}$ can be easily extracted, which is actually $\overline{QR^1} + \overline{QR^2} \pmod 2$. 2) $Decode(\overline{ESQR})$ is the standard decoding operation on $\overline{ESQR}$, which recovers the commitment value com'. 3) $Ver(crs, com', decom, data) = 1$ denotes the opening of commitment com', which is one of the three verifications we proposed.

Here are some details of the triple-verification which can defend against the tampering and forgery attacks on e-coupons. First, the message digest $h(\overline{QR^1})$ is checked under *key* before the recovery of e-coupons. It can verify if $\overline{QR^1}$ is modified, damaged or forged. Then the recovery is achieved and the graph of $\overline{ESQR}$ can be checked. In addition, through opening the commitment, com' is verified. With these three verifications, we cannot only ensure the authenticity and integrity of enhanced QR codes, but also figure out the attacker, i.e., C or S, if any.

Algorithm 4 Recovery

procedure RECOVERY(QR Codes $(\overline{SQR^1}, \overline{SQR^2})$)
  $\overline{ESQR} \leftarrow \overline{SQR^1} + \overline{SQR^2} \pmod 2$
  $com' \leftarrow Decode(\overline{ESQR})$
  if $Ver(crs, com', decom, data) = 1$ **then**
    return (Accept, com')
  end if
return Reject
end procedure

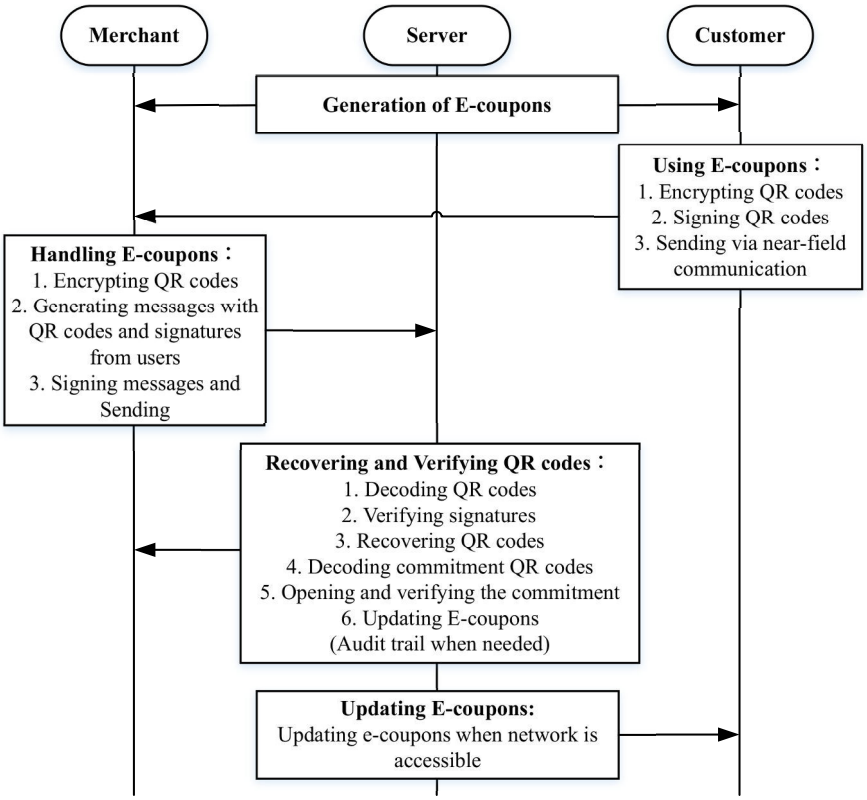

Fig. 4. Protocol flow of EQRC-II

3.5. EQRC-II for Offline Payment

We propose EQRC-II for a scenario where customers visit stores but are not connected to the Internet directly. In this scheme, M will transmit the enhanced QR code from C to S, which results in a new risk, i.e., M may tamper or forge the message from C. Thus we should pay attention to the audit trail of the messages.

The protocol flow of EQRC-II is shown in Fig. 4. The generation and distribution of QR code-based e-coupons in EQRC-II are the same with that in EQRC-I. Other necessary details are provided as follows.

3.5.1. E-coupons Delivery

Similar to EQRC-I, EQRC-II introduces encryption and authentication schemes. $\overline{SQR^1}$ held by C is encrypted first so that M cannot access $\overline{SQR^1}$. The message sent from C to M through near-field communications is $msg_1 = ((\overline{SQR^1})_{pk_S} \parallel \sigma_1)$ where $(\overline{SQR^1})_{pk_S}$ is an encryption result and σ_1 is a signature on $\overline{SQR^1}$ with Algorithm 2. Once receiving msg_1, M computes $m = ((\overline{SQR^1})_{pk_S} \parallel \sigma_1 \parallel (\overline{SRQ^2})_{pk_S})$ which combines msg_1 and the second enhanced QR code. The message sent from M to S is $msg_2 = (m \parallel \sigma_2)$ where σ_2 is a signature on m.

3.5.2. Audit Trail

With the triple-verification scheme, S can verify whether $\overline{SQR^1}$ and $\overline{SQR^2}$ are tampered or forged. However, if $\overline{SQR^1}$ is attacked, S cannot figure out who is the attacker. Thus, we propose an audit trail solution.

When the verification on SQR^1 failed, S submits an audit request to CA who manages the real identities of all users. To prove itself, C needs to connect the Internet and confirm its identity to CA. CA checks if $\sigma_1.T = x \cdot \sigma_1.R + x \cdot sk_C \cdot \sigma_1.S$. The proof is as follows. Note that some transformation is from the join algorithm in [16] which achieves the purpose of certificates, i.e., the credentials in [16].

$$\begin{aligned} \sigma_1.T &= a \cdot C \\ &= a \cdot x \cdot A + a \cdot rxy \cdot pk_C \\ &= a \cdot x \cdot A + a \cdot rxy \cdot sk_C \cdot P_1 \\ &\equiv x \cdot \sigma_1.R + x \cdot sk_C \cdot \sigma_1.S. \end{aligned} \tag{2}$$

If the equation is satisfied, C is the attacker or the data storage of C is compromised. If not, which means σ_1 is not the exact one generated by C, M should be the attacker or the data storage of M needs a strengthened protection.

4. Security Analysis

In this section, we analyze the security of the proposed framework. According to the protocol flow of EQRC, the analyses mainly focuses on the following six aspects.

4.1. Security of the Digital Signature

The security of the digital signature is guaranteed by the hardness of the **blind bilinear LRSW Assumption** [22, 23]. Suppose that a $Setup(1^k)$ algorithm generates the cyclic groups $\mathbb{G}_1 = \langle P_1 \rangle$, $\mathbb{G}_2 = \langle P_2 \rangle$ and $\mathbb{G}_T$ with a prime order q, where k is a parameter related to the security level. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a pairing. Let $X, Y \in \mathbb{G}_2, X = x \cdot P_2, Y = y \cdot P_2$. Let $O_{X,Y}(\cdot)$ denote an oracle that, with a randomly chosen $r \in \mathbb{Z}_q$ and an input $f \in \mathbb{Z}_q$, outputs a triplet (A, B, C) where $A = r \cdot P_1$, $B = y \cdot A$, and $C = (x \cdot A + fxy \cdot A)$. Then given the group setup $(\mathbb{G}_1, \mathbb{G}_2, P_1, P_2, q, \hat{e})$ and the public key (X, Y), it is impossible for a probabilistic polynomial-time (*p.p.t.*) adversary $\mathcal{A}$ to construct the triplet

(A, B, C) without knowing the secret key (x, y). To be specific, for all $\mathcal{A}$, given the security parameter k and the set Q that $\mathcal{A}$ query with $O_{X,Y}(\cdot)$, $v(k)$ is a negligible function defined as follows:

$$\begin{aligned} &Pr[(\mathbb{G}_1, \mathbb{G}_2, P_1, P_2, q, \hat{e}) \leftarrow Setup(1^k); x \leftarrow \mathbb{Z}_q; y \leftarrow \mathbb{Z}_q; X = x \cdot P_2, Y = y \cdot P_2; \\ &(f, A, B, C) \leftarrow \mathcal{A}^{O_{X,Y}}(\mathbb{G}_1, \mathbb{G}_2, P_1, P_2, q, \hat{e}) : f \notin Q \wedge f \in \mathbb{Z}_q \wedge f \neq 0 \wedge A \in \mathbb{G}_1 \wedge B \\ &\qquad = y \cdot A \wedge C = x \cdot A + fxy \cdot A] \leqslant v(k). \end{aligned} \tag{3}$$

This assumption guarantees that without the secret key (x, y) and the random number $r \in \mathbb{Z}_q$, any *p.p.t.* adversary cannot forge a valid credential (A, B, C). Furthermore, for the case of the signing algorithm, a signature σ is constructed with the secret parameters a and z, the user's secret key sk_U (i.e., sk_C or sk_M), the timestamp n_t and the shuffled credential (R, S, T) where $R = a \cdot A$, $S = a \cdot B$, and $T = a \cdot C$. Any adversary $\mathcal{A}$ cannot produce a valid anonymous signature σ for any message msg without (A, B, C) and sk_U. Thus, a signed message cannot be forged or modified during the processes of transmission, which provides the non-repudiation, authenticity and integrity of messages. In addition, because there is no isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$ in the asymmetric pairing setting [24], it is infeasible to link (R, S, T) to the original (A, B, C) without the secret parameter a, which provides users with anonymity.

For the case of the verification algorithm, the above assumption also guarantees that only holding the bilinear group parameters $(\mathbb{G}_1, \mathbb{G}_2, P_1, P_2, q, \hat{e})$, the public key (X, Y), the message msg, and the shuffled credential (R, S, T), users can check whether the following verification equations hold: $\hat{e}(A, Y) = \hat{e}(B, P_2)$, $\hat{e}(A, X)\hat{e}(fB, X) = \hat{e}(C, P_2)$, $\hat{e}(R, P_2) = \hat{e}(A, P_2)^a$, $\hat{e}(S, P_2) = \hat{e}(A, Y)^a$, and $\hat{e}(T, P_2) = \hat{e}(A, X)^a\hat{e}(fB, X)^a$.

4.2. Security of the Encryption

The security of the ElGamal encryption in this work is guaranteed by the hardness of the **Decisional Diffie-Hellman (DDH) Assumption** [15]: Assume that $\mathbb{G}_1 = \langle P_1 \rangle$, $\mathbb{G}_2 = \langle P_2 \rangle$ and $\mathbb{G}_T$ are cyclic groups with a prime order q. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a pairing. Let $X, Y, Z \in \mathbb{G}_1$, $X = x \cdot P_1$, $Y = y \cdot P_1$, and $Z = z \cdot P_1$. Note that x, y and z are randomly and independently chosen from $\mathbb{Z}_p$. Then given the group parameters $(\mathbb{G}_1, \mathbb{G}_2, P_1, P_2, q, \hat{e})$, for any probabilistic-polynomial time $(p.p.t.)$ adversary $\mathcal{A}$, the advantage $\mathbf{Adv}_{\mathcal{A}}^{DDH}$ defined as follows is negligible:

$$\begin{aligned} \mathbf{Adv}_{\mathcal{A}}^{DDH} = |&Pr[x, y, z \leftarrow \mathbb{Z}_q; X = x \cdot P_1, Y = y \cdot P_1, Z = z \cdot P_1; \mathcal{A}(\mathbb{G}_1, \mathbb{G}_2, \\ &P_1, P_2, X, Y, Z, q) = 1] - Pr[x, y \leftarrow \mathbb{Z}_q; X = x \cdot P_1, Y = y \cdot P_1, Z = \mathbb{G}_1; \\ &\mathcal{A}(\mathbb{G}_1, \mathbb{G}_2, P_1, P_2, X, Y, Z, q) = 1]|. \end{aligned} \tag{4}$$

In other words, the distributions $\langle x \cdot P_1, y \cdot P_1, xy \cdot P_1 \rangle$ and $\langle x \cdot P_1, y \cdot P_1, z \cdot P_1 \rangle$ are computationally indistinguishable, which is equivalent to the semantic secure in ElGamal encryption [24]. This assumption guarantees that, without knowing the private key, the probability of getting $z = xy$ from $Z = xy \cdot P_1$ for a *p.p.t.* adversary $\mathcal{A}$ is negligible. Thus, the confidentiality of messages in transmission is provided in our framework. As summarized in Table 3, the typical attacks on e-coupons and messages transmitted, including the data leakage, forgery and modification, are resisted.

4.3. Security of the Commitment

In general, there are three algorithms in a **Pedersen commitment** [17, 25], i.e., the generation algorithm $\texttt{Gnrt}$, the commitment algorithm $\texttt{Comm}$ and the opening algorithm $\texttt{Opnv}$. Let k denote the security parameter. Suppose that the $\texttt{Gnrt}(1^k)$ algorithm generates a set of common parameters (p,q,g,h) as follows: p and q are two primes which are large enough and $q|p-1$. g and h are generators randomly chosen from a q-order subgroup $\mathbb{G}_q$ of $\mathbb{Z}_p^*$. $h = g^a \mod p$ where a is secret. On inputting a secret $m \in \mathbb{Z}_q$ and a random value $r \in \mathbb{Z}_q$, the $\texttt{Comm}$ algorithm computes a commitment $com = \texttt{Comm}(m,r) = g^m h^r \mod p$, where $com \in \mathbb{Z}_p^*$. Based on the DLP, $\log_g h$ is unknown to the committer. Correspondingly, given a commitment com, a message $m \in \mathbb{Z}_q$ and $r \in \mathbb{Z}_q$, the $\texttt{Opnv}(com,m,r)$ algorithm will output $TRUE$ if and only if com is a valid commitment to m with the given r.

Based on the design described above, for any given value r, the commitment is uniformly distributed with a randomly and uniformly chosen parameter [17], i.e., $|\Pr[\texttt{Com}(m_1,r)] - \Pr[\texttt{Com}(m_2,r)]| = 0$, where $m_1, m_2, r \in \mathbb{Z}_q$ and r follows the uniform distribution. In other words, given a commitment com, every value m is equally likely to be the value committed in com. This property is well-known as the **Perfect Hiding Property**.

In EQRC, the perfect hiding property provided by Pedersen commitment guarantees that any adversary on the channel can only obtain data from $\overline{QR}$ with a negligible probability. To be specific, for every sensitive data $data$ in $\overline{QR}$, there exists a unique $data'$ such that $com = g^{data} h^{r_1} = g^{data'} h^{r_2}$. Thus, com perfectly hides all information about $data$, i.e., the adversary cannot get any advantage from com to guess $data$, even with unlimited computational power. Note that the commitment provides additional protection with the QRFC approach. Even both the two fragments $\overline{SQR^1}$ and $\overline{SQR^2}$ are intercepted and $\overline{QR}$ is recovered, $data$ is still safe. Thus, the commitment technology adopted in EQRC resists against not only the data leakage, forgery and modification attacks on e-coupons, but also the collusion attack between M and C, as in Table 3.

In addition, we introduce the **Non-ambiguity Property** to prove that it is infeasible for a *p.p.t.* adversary $\mathcal{A}$ to forge a different commitment in other ways [26]. To be specific, the advantage $\mathbf{Adv}_{\mathcal{A}}^{NAmb}$ of $\mathcal{A}$ defined as follows is negligible:

$$\begin{aligned} \mathbf{Adv}_{\mathcal{A}}^{NAmb} = Pr[(g,h,q,p,p^*) \leftarrow \texttt{Gnrt}^*(1^k); r, r^*, m \leftarrow \mathbb{Z}_q; \\ (com, r, r^*) \leftarrow \texttt{Comm}^*(\mathbb{G}_q, g, h, p^*, m); \\ \texttt{Opnv}(p, com, r) \neq \perp, \texttt{Opnv}(p, com, r^*) \neq \perp, \\ \texttt{Opnv}(p, com, r) \neq \texttt{Opnv}(p, com, r^*)], \end{aligned} \tag{5}$$

where $\texttt{Gnrt}^*$ and $\texttt{Comm}^*$ are the generation and the commitment algorithms launched by $\mathcal{A}$.

4.4. Security of the HMAC

For one thing, the security of HMAC is provided by the common construction defined as follows: $HMAC(K,m) = H((K' \oplus opad)||H((K' \oplus ipad)||m))$, where m is a message, K is a secret key, K' is a block-sized key derived from K, $opad$ and $ipad$ are the block-sized outer and inner padding respectively, and H is a hash function. In such a construction, the application of the outer function H masks the intermediate result of the internal $H((K' \oplus ipad)||m)$ [27–29]. Additionally, the cryptographic strength

of HMAC depends on the properties of the underlying hash function. In our framework, we adopt SHA-2, which uses the **Merkle-Damgåd Structure**. The soundness of the Merkle-Damgåd structure has been proved [30], that is, if the compress function $f : \{0,1\}^{m+n} \rightarrow \{0,1\}^m$ is collision resistant, then the constructed hash function h is collision resistant. In SHA-2, the compress function h_{DM} is designed from a block cipher $\{f_k\}$ using **Davies-Meyer Construction** $h_{DM}(k,x) = f_k(x) \oplus x$, where k and x are inputs of the model. Collision resistance of Davies-Meyer construction can be proved in the ideal-cipher model [31].

Based on the discussion above and the existing research [32], the security of SHA-2 has been widely analyzed and proved. Theoretically, taking SHA-256 as an example, the upper bound of finding a collision using the birthday attack is 2^{128} evaluations and that of a preimage attack using a brute force search is 2^{256}. Though there are some research efforts aiming at attacks [33–35], it is still widely accepted that SHA-2 family is a secure hash algorithm.

Overall, in QRFC, as only the Server S knows the HMAC key *key*, both the origin authentication and data integrity for $\overline{QR^1}$ are provided based on the security of HMAC-SHA-2.

4.5. Security of the QRFC Approach

Because of the pseudorandomness property of the PRNG algorithm, the output sequences are computationally indistinguishable for any *p.p.t.* algorithm $\mathcal{A}$, i.e., for all sufficiently large n and positive polynomial $p(\cdot)$, we have

$$\left|Pr[\mathcal{A}(\mathcal{G}(U_n)) = 1] - Pr[\mathcal{A}(U_{l(n)}) = 1]\right| < \frac{1}{p(n)}. \tag{6}$$

$\mathcal{G}$ is a PRNG with an output length $l(n)$, U_n is the uniform distribution on $\{0,1\}^n$ and $U_{l(n)}$ on $\{0,1\}^{l(n)}$. The pseudorandomness property guarantees that when $\overline{QR}$ is re-encoded to $\overline{QR^1}$ and $\overline{QR^2}$ by the QRFC approach, the choice for any block is pseudorandom. Anyone with a single enhanced QR code can only guess $\overline{QR}$ with a 0.5^n probability of success, where n is the number of blocks in $\overline{QR}$. In our framework, each user, i.e., M or C can only hold one of the pair $(\overline{SQR^1}, \overline{SQR^2})$. Thus, the confidentiality and integrity of $\overline{QR}$ are provided as it is hard for M or C to recover $\overline{QR}$ by itself. In other words, the data leakage, forgery and modification attacks on e-coupons can be resisted, which is summarized in Table 3.

4.6. Security of the Triple Verification

The security of the first verification is guaranteed by the HMAC-SHA-2, as we analyze in Section 4.4. The secure hash $h(QR^1)$ stored in $\overline{CQR}$ is produced with *key*. Thus no one without *key* can recompute the hash while tampering or forging $\overline{SQR^1}$. Then, the security of the second verification is based on the design of the enhanced QR code. Tampering on one of the enhanced QR codes may lead to anomaly in the process of recovery. See section 3.4, for example, the carrier QR code may not change to all black. The third verification is commitment opening, with which S can check *com* to guarantee the integrity and authenticity of the sensitive data in e-coupons. The detailed analysis is given in Section 4.3. The triple verification works together to ensure the security of our framework. Note that if an attack is detected by the first verification, it shows that the attack source is C, i.e., C is an attacker itself, or there are risks of the data storage or transmission in C. Otherwise, the attack source is M.

Table 3
Defense Against the Attacks

Defense	Signing	Encryption	Commitment	QRFC	Verify	Timestamp
Data Leakage		✓	✓	✓		
E-coupon Forgery and Modification		✓	✓	✓	✓	
Collusion Attack			✓		✓	
Eavesdropping		✓				
Message Forgery and Modification	✓	✓				
Message Replay						✓

The defense mechanisms against the attacks are summarized in Table 3. Note that *Verify* denotes the triple-verification.

5. Performance Evaluation

In this section, we analyze the efficiency of the signature scheme, the overhead of enhanced QR codes, and the communication overhead. All experiments are conducted on Windows 8, with 2.8 GHz Intel CPU, 12 GB memory and 500 GB disk.

5.1. Computation Overhead of the Signature Scheme

We consider the scalar multiplications in $\mathbb{G}_1$, the exponentiations in $\mathbb{G}_t$ and pairing operations, which are time costly operations. The hash operations in $\mathbb{Z}_q$ can be neglected with little overhead. The exponentiations in $\mathbb{G}_t$ can be converted into the scalar multiplications in $\mathbb{G}_1$ to reduce the computation complexity [15]. Thus the computation overhead for signature is determined by $4 \cdot \mathbb{G}_1 + 1 \cdot P$ and that for verification is $3 \cdot \mathbb{G}_1 + 5 \cdot P$, where $n \cdot \mathbb{G}_1$ represents the n scalar multiplications on $\mathbb{G}_1$, and $m \cdot P$ is m pairing operations on $\mathbb{G}_t$.

The experiment in [36] shows that we need to set $|q| = 160$ bits and $|\mathbb{G}_1| = 161$ bits to meet the 80-bit security level. Then one scalar multiplication in $\mathbb{G}_1$ costs 0.6 ms and one exponentiation in $\mathbb{G}_t$ costs 4.5 ms [16]. In our work, the computation overhead for signing and verification is 6.9 ms and 24.3 ms, respectively. Compared with the experiment in [36], the signing in our work is better than that in TAA V1 [16], TAA V2 [16] and GSIS [37]. Because we do not consider the pre-computing of pairing operations, the verification efficiency is lower than that in GSIS, i.e., 13.8 ms.

5.2. Encoding/Decoding Overhead for the Enhanced QR Codes

In our framework, the generation, recovery and verifications of the enhanced QR codes are realized by S with cloud computing, which significantly reduces the computation burden of users.

We evaluate the time consumption for QRFC approach, which is developed based on C#. Three different versions of QR codes are tested, which are Version 1 (Block 21×21), Version 3 (Block 25×25) and Version 7 (Block 33×33). The samples of QR codes are shown in Table 4, where the QR codes with similar pixel resolutions (e.g., for mobile phones or posters) are given the same labels.

The running-time overhead for the encoding process in QRFC is calculated from two stages: the preprocessing stage and the computing stage. The preprocessing stage includes the processes such as

Table 4
The Setting of QR Code Samples

	a1	a2	a3	b1	b2	b3	c1	c2	c3
Block	Version 1: 21 × 21			Version 3: 25 × 25			Version 7: 33 × 33		
Graph Length (Pixel)	105	210	294	100	200	300	99	198	297
Size (KB)	1.70	5.80	11.5	1.62	5.52	11.7	1.60	5.47	11.6

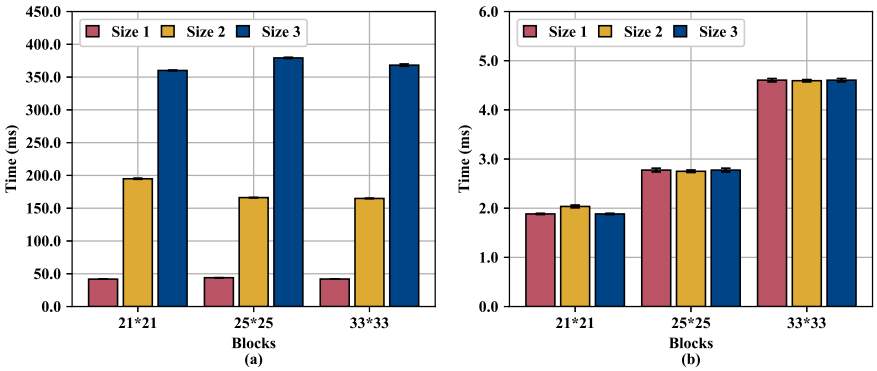

Fig. 5. Running-time overhead for encoding in (a) the preprocessing stage and in (b) the computing stage

reading the QR codes and building Bitmap objects with C#. The overhead for the preprocessing stage is shown in Fig. 5(a) and that for the computing stage is shown in Fig. 5(b). We can see that the version of QR codes has little effect on the preprocessing time but the size of QR codes affects a lot. Compared with the preprocessing stage, the overhead for the computing stage is trivial. Therefore the encoding time is mainly determined by the preprocessing stage, which is the same for all schemes regardless security.

On the other hand, the decoding process for QRFC also contains two parts: the preprocessing stage and the computing stage. The overhead of the preprocessing stage is shown in Fig. 6(a). The overhead of the computing stage which includes the processes of decoding computation and original QR codes recovery is shown in Fig. 6(b). It is clear that the computing stage costs less time. Comparing the decoding process with the encoding process, we can find that the decoding process is more efficient, costing less time than the encoding process, which is better for e-coupon transactions.

5.3. Communication Overhead

To evaluate the communication overhead, we implemented a simulation on the end-to-end delay from users to a server. The experiment is conducted by a well-known simulation tool, OMNeT++ 5.5 [38]. An open-source OMNeT++ model suite, INET [39], is adopted.

The network is designed as shown in Fig. 7. The host denotes users in our system, which can be clients or merchants. The hosts are connected to an access point, AP, via a wireless network and thus can send messages to the server through a wired core network. Considering the networking technologies nowadays, we choose IEEE802.11ac with a bit rate of 346.7 Mbps as the wireless network to ensure that most of the new mobile devices can support [40, 41]. The bit rate of the wired network is set as 1000 Mbps with a packet drop rate of 1%. The maximum propagation delay is calculated as the ratio between the half of the longest distance from east to west Canada (2757 km) [42] and the light speed for optical

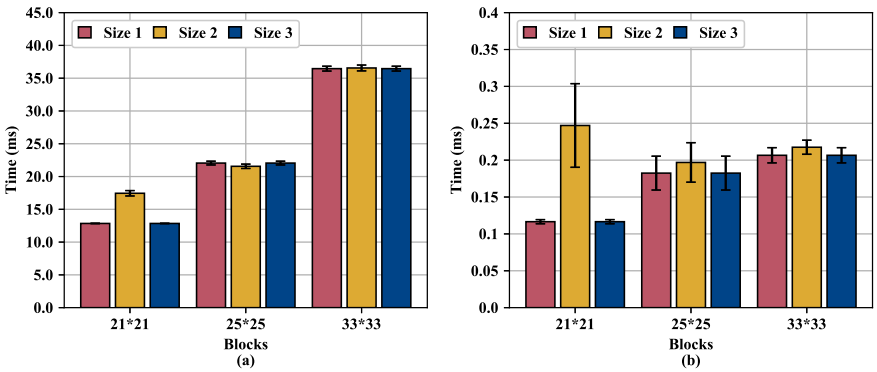

Fig. 6. Running-time overhead for decoding in (a) the preprocessing stage and in (b) the computing stage

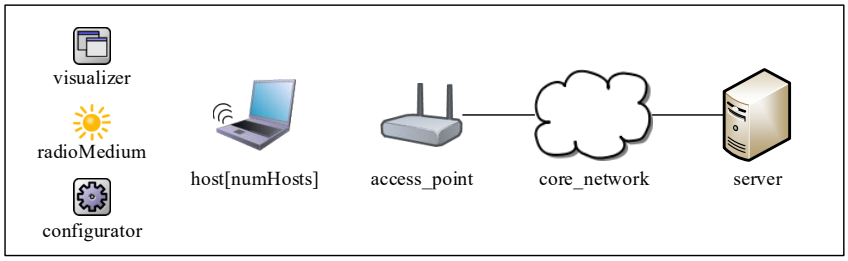

Fig. 7. Network design in Omnet++

cables (180 000 km/s), which is 15.3167 ms. Note that the server is deployed on the cloud and thus can handle the requests via cloud computing, which is not the main consideration of this simulation.

In this simulation, we mainly focus on the messages sent from users to servers which are the signatures and the ciphertext of $\overline{SQR^1}$ or $\overline{SQR^2}$. The size of a signature is $|\sigma| = 3|\mathbb{G}_1| + 3|q|$. A 160-bit long prime number q and a 161-bit long group $\mathbb{G}_1$ are selected in order to meet the security level of the standard 1024-bit RSA. Therefore the size of a signature is close to 1 kb. The ciphertext in the ElGamal scheme doubles the size of the plaintext, i.e., $\overline{SQR^1}$ or $\overline{SQR^2}$.

The size of enhanced QR codes is variable in different settings. For example, as the size of *com* and *data* is no larger than 160 bits, a version-3 QR code is able to encode them with an H-level ECC (Error Correction Capability). Thus, there are 29×29 blocks in $\overline{QR}$. To reduce the QR codes size, we use one pixel in each block. Then the 841 bits need $841 \times 4 = 3364$ bits to represent with the QRFC approach, i.e., each of the $\overline{QR^1}$ and $\overline{QR^2}$ is 3364 bits. If we embed the split QR codes into a carrier QR code with an L-level ECC, which can tolerate only 7% errors, the size of each enhanced QR codes generated is $3364/0.07 = 48058$ bits. Note that the split QR codes embedded are treated as errors by a regular decoder as described in Section 3.2.3. Thus, if the carrier QR codes are smaller than the bound, it cannot be read by a regular decoder with error correction. Overall, a single communication with the settings above should have about 12 KB in EQRC-I, and 24 KB in EQRC-II where a merchant sends two enhanced QR codes. Some typical message lengths are listed in Table 5.

Table 5
Typical Message Length

Version†	ECC‡ ($\overline{QR}$)	ECC ($\overline{CQR}$)	Size§	Length¶ (EQRC-I)	Length¶ (EQRC-II)
2	Q	H	1.04	2.08	4.16
3	H	H	1.4	2.8	5.6
3	H	Q	1.68	3.36	6.72
2	Q	L	4.46	8.92	17.84
3	H	L	6	12	24

† The versions chosen for $\overline{QR}$. Each version has a different module configuration or number of modules [43]. ‡ Four levels are available for different QR code error correction capabilities: Level L (7%), Level M (15%), Level Q (25%) and Level H (30%) [44]. § The size for one enhanced QR code (KB). ¶ Approximate length of each message (KB).

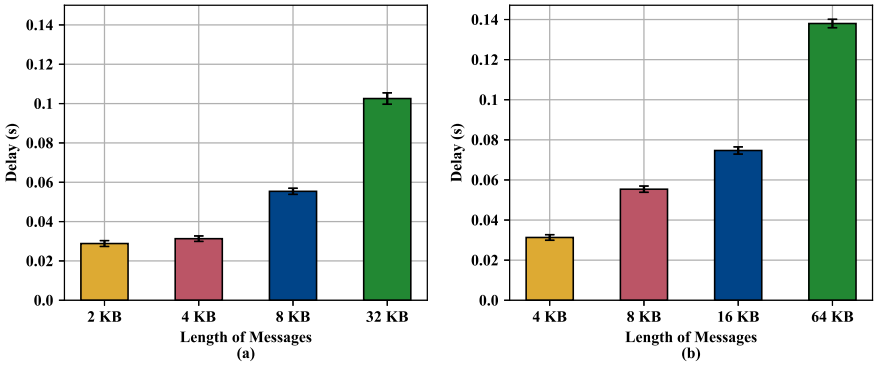

Fig. 8. End-to-end delay in (a) EQRC-I and in (b) EQRC-II

To measure the effect of the message length on the end-to-end delay, we set the message length as 2, 4, 8 and 32 KB for EQRC-I and doubled the size for EQRC-II. In the experiment, 100 messages are sent following a Poisson process in 100 s, which simulates a common scenario with request intensity of 1 (per second). Note that, too large QR codes are seldom used in real life, but we also measure the delay with a rare message length of 32 KB in EQRC-I and 64 KB in EQRC-II, when the latest QR code version (40) is adopted as $\overline{CQR}$. The results are shown in Fig. 8. We can see that, the average end-to-end delay is mainly bounded by 0.1 s. Even with the rare size of enhanced QR codes, the delay is also acceptable.

To measure the effect of the scale of users on the end-to-end delay, we set the number of hosts in the simulation as 100, 500, 1000 and 1500. Each host is expected to send only one 4-KB message with an inter-arrival time following the exponential distribution [45]. The service time is set as 100 s to represent normal scenarios such as using coupons in a shopping mall. In other words, the request intensity is set as 1, 5, 10 and 15 per second. The intensity set is expected to have little influence on the end-to-end delay, otherwise, the system capacity is reached easily even in a normal scenario. Besides, another experiment is conducted where all messages are sent at the same time to test the performance further. The variable, number of requests, is set as 100 and 500. In such a burst, the delay is expected to be larger but in an acceptable range. The results in Fig. 9 are the same with the reasonable expectation. It indicates that the delay is not affected much by the scale of requests in normal scenarios while is larger in a burst.

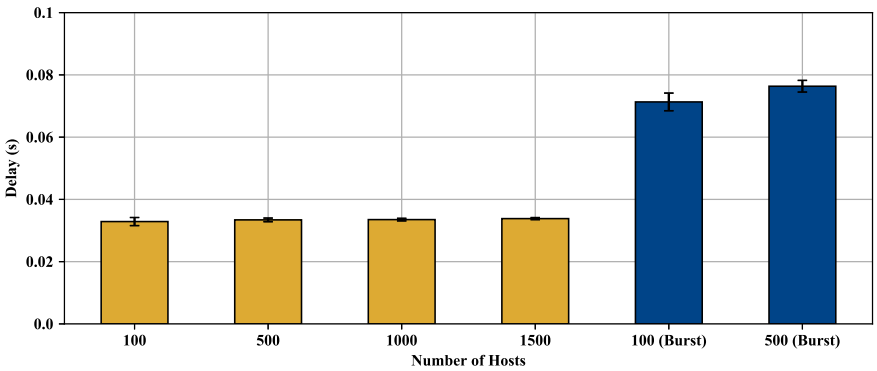

Fig. 9. End-to-end delay in normal scenarios (yellow) and in a burst (blue)

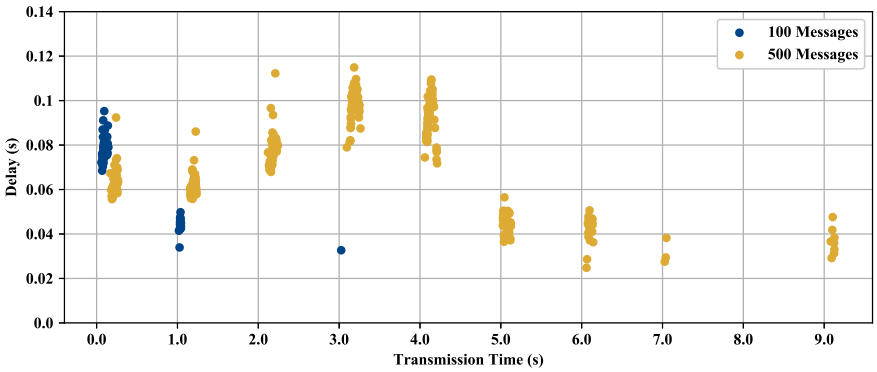

Fig. 10. End-to-end delay and the transmission time in a burst

Fig. 10 shows the transmission time of each message and the corresponding delay in bursts. It is clear that when there are 100 hosts trying to send QR codes at the same time, most of the requests are sent out directly and some succeed in around 1 second because of the collisions at the AP. Only a few wait for 3 seconds. When there are 500 hosts, the upper bound of waiting time is around 9 seconds. Overall, with the network configuration described in this section, the EQRC performance is good and acceptable even with a burst.

6. Conclusion

In this paper, we first proposed a fragment-based approach to enhance the confidentiality of QR codes. Second, we designed an enhanced QR code scheme with the combination of the QRFC approach and the commitment technique. The enhanced QR code scheme can prevent the leakage of the sensitive information in QR codes and forgery or tampering of QR codes. Third, we gave a secure e-coupon transaction framework called EQRC based on the techniques above. EQRC provides a triple-verification mechanism, reducing the security threats during the e-coupon delivery and transaction. Both online and offline scenarios are supported by EQRC, which provides a comprehensive protection for the real situation.

The strong analyses and evaluation have shown that the proposed framework has a high security and low computing and communication overhead.

In the future, we will research in the following aspects:

(1) The colored QR codes have more storage space. Thus, using colored QR codes to implement the fragment coding of QR codes, will be an attractive research direction in the future.
(2) A recently developed QR code called Frame QR has a region where the arbitrary altering of figures and contents will not affect other regions. Combining Frame QR into the design of our EQRC can make the generation and merging of enhanced QR codes more standardized and concise.
(3) An illegitimate copy on e-coupons has the potential to infringe the rights of legitimate holders. The current method in EQRC is to check the freshness. It is feasible to consider both the copy prevention and detection solutions acting on QR codes directly.

References

[1] R. Liu, J. Song, Z. Huang and J. Pan, EQRC: An enhanced QR code-based secure e-coupon transaction framework, in: *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, IEEE, 2019, pp. 1–6.
[2] F. Cadger, K. Curran, J. Santos and S. Moffett, A survey of geographical routing in wireless ad-hoc networks, *IEEE Communications Surveys & Tutorials* **15**(2) (2013), 621–653.
[3] A. Kharraz, E. Kirda, W. Robertson, D. Balzarotti and A. Francillon, Optical delusions: a study of malicious QR codes in the wild, in: *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, IEEE, 2014, pp. 192–203.
[4] K. Krombholz, P. Frühwirt, T. Rieder, I. Kapsalis, J. Ullrich and E. Weippl, QR code security—How secure and usable apps can protect users against malicious QR codes, in: *2015 10th International Conference on Availability, Reliability and Security*, IEEE, 2015, pp. 230–237.
[5] V. Mavroeidis and M. Nicho, Quick response code secure: a cryptographically secure anti-phishing tool for QR code attacks, in: *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, Springer, 2017, pp. 313–324.
[6] X. Zhang, H. Li, Y. Yang, G. Sun and G. Chen, LIPPS: Logistics information privacy protection system based on encrypted QR code, in: *Trustcom/BigDataSE/ISPA*, IEEE, 2016, pp. 996–1000.
[7] S. Sharma and V. Sejwar, Impementation of QR code based secure system for information sharing using Matlab, in: *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, IEEE, 2016, pp. 294–297.
[8] Y. Cheng, Z. Fu and B. Yu, Improved visual secret sharing scheme for QR code applications, *IEEE Transactions on Information Forensics and Security* **13**(9) (2018), 2393–2403.
[9] P. Lin and Y. Chen, High payload secret hiding technology for QR codes, *EURASIP Journal on Image and Video Processing* **2017**(1) (2017), 14–21.
[10] I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J. Gaudin and C. Guichard, Two-level QR code for private message sharing and document authentication, *IEEE Transactions on Information Forensics and Security* **11**(3) (2016), 571–583.
[11] C. Zhang, X. Lin, R. Lu, P. Ho and X. Shen, An efficient message authentication scheme for vehicular communications, *IEEE Transactions on Vehicular Technology* **57**(6) (2008), 3357–3368.
[12] C. Lee and Y. Lai, Toward a secure batch verification with group testing for VANET, *Wireless Networks* **19**(6) (2013), 1441–1449.
[13] R. Hasan, R. Sion and M. Winslett, The case of the fake picasso: preventing history forgery with secure provenance., in: *FAST*, Vol. 9, 2009, pp. 1–14.
[14] E. Brickell, J. Camenisch and L. Chen, Direct anonymous attestation, in: *Proceedings of the 11th ACM Conference on Computer and Communications Security*, ACM, 2004, pp. 132–145.
[15] L. Chen, P. Morrissey and N.P. Smart, DAA: Fixing the pairing based protocols, *Cryptology ePrint Archive* (2009).
[16] L. Chen, S. Ng and G. Wang, Threshold anonymous announcement in VANETs, *IEEE Journal on Selected Areas in Communications* **29**(3) (2011), 605–615.
[17] T.P. Pedersen, Non-interactive and information-theoretic secure verifiable secret sharing, in: *Annual International Cryptology Conference*, Springer, 1991, pp. 129–140.
[18] D. Jena and S.K. Jena, A novel visual cryptography scheme, in: *2009 International Conference on Advanced Computer Control*, IEEE, 2009, pp. 207–211.

[19] M. Naor and A. Shamir, Visual cryptography, in: *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, 1994, pp. 1–12.
[20] O. Goldreich, *Foundations of Cryptography*, Cambridge University Press, 2007.
[21] M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudorandom bits, *SIAM Journal on Computing* **13**(4) (1984), 850–864.
[22] L. Zhang, J. Song and J. Pan, A privacy-preserving and secure framework for opportunistic routing in DTNs, *IEEE Transactions on Vehicular Technology* **65**(9) (2015), 7684–7697.
[23] A. Lysyanskaya, R.L. Rivest, A. Sahai and S. Wolf, Pseudonym systems, in: *International Workshop on Selected Areas in Cryptography*, Springer, 1999, pp. 184–199.
[24] Y. Tsiounis and M. Yung, On the security of ElGamal based encryption, in: *International Workshop on Public Key Cryptography*, Springer, 1998, pp. 117–134.
[25] Wikstr and M. Douglas, A commitment-consistent proof of a shuffle, in: *Information Security & Privacy, Australasian Conference, Australia,*, 2009.
[26] S. Halevi, Efficient commitment schemes with bounded sender and unbounded receiver, in: *Annual International Cryptology Conference*, Springer, 1995, pp. 84–96.
[27] H. Krawczyk, M. Bellare and R. Canetti, HMAC: Keyed-hashing for message authentication, Technical Report, 1997.
[28] S. Kelly and S. Frankel, Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, Technical Report, 2007.
[29] S. Turner and L. Chen, Updated security considerations for the MD5 message-digest and the HMAC-MD5 algorithms, Technical Report, 2011.
[30] I.B. Damgård, A design principle for hash functions, in: *Conference on the Theory and Application of Cryptology*, Springer, 1989, pp. 416–427.
[31] J. Black, P. Rogaway and T. Shrimpton, Black-box analysis of the block-cipher-based hash-function constructions from PGV, in: *Annual International Cryptology Conference*, Springer, 2002, pp. 320–335.
[32] H. Gilbert and H. Handschuh, Security analysis of SHA-256 and sisters, in: *International Workshop on Selected Areas in Cryptography*, Springer, 2003, pp. 175–193.
[33] F. Mendel, T. Nad and M. Schläffer, Improving local collisions: new attacks on reduced SHA-256, in: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2013, pp. 262–278.
[34] M. Eichlseder, F. Mendel and M. Schläffer, Branching heuristics in differential collision search with applications to SHA-512, in: *International Workshop on Fast Software Encryption*, Springer, 2014, pp. 473–488.
[35] C. Dobraunig, M. Eichlseder and F. Mendel, Analysis of SHA-512/224 and SHA-512/256, in: *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2015, pp. 612–630.
[36] M. Scott, *Efficient implementation of cryptographic pairings*, 2007. http://www.pairing-conference.org/2007/invited/Scottslide.pdf.
[37] X. Lin, X. Sun, P.-H. Ho and X. Shen, GSIS: A secure and privacy-preserving protocol for vehicular communications, *IEEE Transactions on Vehicular Technology* **56**(6) (2007), 3442–3456.
[38] *OMNeT++*. https://omnetpp.org.
[39] *INET Framework*. https://inet.omnetpp.org.
[40] R. Tarabuţă, D. Balan, A. Potorac and A. Graur, Performance investigation over 802.11 ac communication environment, in: *2016 22nd International Conference on Applied Electromagnetics and Communications (ICECOM)*, IEEE, 2016, pp. 1–5.
[41] E. Lopez Aguilera, E. Garcia Villegas and J. Casademont, Evaluation of IEEE 802.11 coexistence in WLAN deployments, *Wireless Networks* **25**(1) (2019), 87–104.
[42] *Geography - Statistics Canada*, 2016. https://www150.statcan.gc.ca/n1/pub/11-402-x/2012000/chap/geo/geo-eng.htm.
[43] D. Wave, Information technology automatic identification and data capture techniques QR code bar code symbology specification, *International Organization for Standardization, ISO/IEC* **18004** (2015).
[44] V. Hajduk, M. Broda, O. Kováč and D. Levickỳ, Image steganography with using QR code and cryptography, in: *2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA)*, IEEE, 2016, pp. 350–353.
[45] X. Nan, Y. He and L. Guan, Optimal resource allocation for multimedia cloud based on queuing model, in: *2011 IEEE 13th International Workshop on Multimedia Signal Processing*, IEEE, 2011, pp. 1–6.

View Reviewer Comments for Manuscript
JCS-191416
"EQRC: A Secure QR Code-based E-coupon Framework Supporting Online and Offline Transactions"

Click the Reviewer recommendation term to view the Reviewer comments.

	Original Submission
Yesi Novaria Kunang, M.Kom. (Reviewer 1)	Accepted pending minor revisions
(Reviewer 2)	Accepted pending minor revisions
(Reviewer 3)	Accepted pending minor revisions
Author Decision Letter	Revise and resubmit pending major revisions
Author	Response to Reviewers