A QR Symbol with ECDSA for Both Public and Secret Areas using Rhombic Sub-cells

Nobuyuki TERAURA[1], Isao ECHIZEN[2] and Keiichi IWAMURA[3]
[1]Terrara Code Research Institute, Tokai, Japan
E-mail: nobu@tcodes.jp Tel: +81-562-74-5378
[2]National Institute of Informatics, Tokyo, Japan
E-mail: iechizen@nii.ac.jp Tel: +81-3-4212-2000
[3]Tokyo University of Science, Tokyo, Japan
E-mail: iwamura@ee.kagu.tus.ac.jp Tel: +81-3-5876-1717

***Abstract*— QR codes have a public data area that anyone can read. However, if there was a secret data area that could be read with only a specific reader, their application range could be greatly expanded. Anyone can create a QR code, so QR codes are easy to spoof or forge. A potential countermeasure is to implement a digital signature in the symbol. For a QR code to be able to safely transfer both secret and public data, it needs three independent data areas: a public data area, a secret data area, and a digital signature area. To meet this requirement, we propose using a QR symbol with a rhombic sub-cell structure that has a central sub-cell part and a lattice sub-cell part. Public data is stored in the central sub-cell part, and a digital signature is stored in the lattice sub-cell part. Secret data is encrypted using the recipient's elliptic function public key and stored in a data area created using double encoding. A digital signature is created that covers both the public data and encrypted secret data, making it possible to safely transfer secret data in addition to public data.**

I. INTRODUCTION

QR codes [1] can be easily created by anyone, and anyone can easily read the data using a smartphone. Since they are easy to create, they are easy to spoof or forge. At the minimum level of security, the creator may be known. In addition, since they are easy to read, secret data cannot be stored in them. However, if secret data could be accommodated with QR codes, the range of their application could be expanded since there is a great need for transfer secret data.

Digital signatures have been implemented in QR codes for various purposes. For example, a digital signature could be used to authenticate the creator [2] [3]. In addition, various hand proposals have been made regarding the transfer of secret data [4]. The elliptic curve digital signature algorithm (ECDSA) has actually been implemented in the normal data section [5] [6] [7] [8]. The normal QR code is used as is, and, in addition to the data required for the application, the ECDSA data is written in the data part. A data area separate from the normal data part could be created for implementing a digital signature separately from the application data [9] [10]. The RSA digital signature could be implemented in the unused area (padding area) of the QR code data area [9], or the ECDSA digital signature could be XORed and embedded in the error correction data area of the QR code [10].

We previously proposed using a rhombic sub-cell to embed a digital signature in a symbol [11]. Also proposed was a method for embedding data encrypted with a common key in an unused area (filled area) of the QR code data area [12] and a method for encrypting a newly generated data area in a color QR symbol [13].

We proposed implementing the ECDSA using rhombic sub-cells and did not consider the implementation of secret data [11]. In this paper, we propose using the rhombic sub-cell structure QR symbol [11] and storing secret data in a data area created by double coding. Attaching a digital signature to the secret data in addition to the public data would prevent forgery and tampering.

Then, we propose an algorithm that adds confidential data by double coding of the public area and the electronic signature area, and adds an digital signature to the public data and the secret data.

In this paper, we call a two-dimensional symbol that conforms to the ISO/IEC international standard [1] a "QR code" and a two-dimensional symbol that is compatible with a QR code but has different specifications a "QR symbol."

II. PROPOSED METHOD FOR STORING SECRET DATA

A. QR symbol threat and effect of digital signature

The four major threats to information security are eavesdropping, spoofing, tampering, and denial. The correspondence between these threats and the threats to a QR symbol is shown in the left column of Table 1. Eavesdropping corresponds to reading secret data, and spoofing corresponds to forgery, duplication, and copying. As shown in the rightmost column, the effect of a digital signature on these threats is the prevention of forgery, falsification, and denial.

Table 1 QR symbol threats and effect of digital signature

Threat		Digital signature
Communication	QR symbol	
Eavesdropping	Read secret data	—
Spoofing	Forgery	○
	Duplication	—
	Copy	—
Tampering	Data change	○
Denial		○

B. *Remaining challenges*

Our proposed method is aimed at dealing with the threats not addressed by a digital signature.

(1) Reading secret data
(2) Copying symbol
(3) Duplicating symbol

Therefore, this paper is an extension of [11]. This extension makes it possible to deal with all threats of QR symbols.

(1) Reading secret data

The secret data is stored in a data area created using double coding, as described later. As shown in Fig. 1, the secret data is encrypted using the public key of the person who is authorized to read the secret data and is decrypted with the private key of the authorized reader. The ID of the public key used for encryption is stored in the embedded area of the public data area, enabling the corresponding private key to be specified.

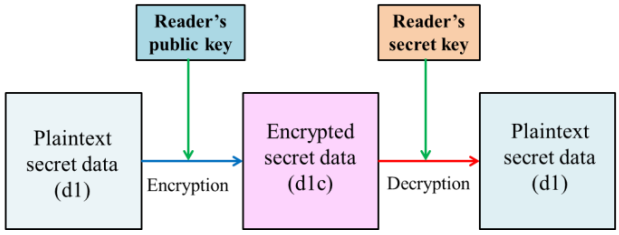

Fig. 1 Encryption and decryption of secret data

(2) Copying symbol

Copying a symbol means copying a regular QR symbol with a copy machine. Therefore, the printed QR symbol is the target. This is prevented by double encoding the secret data using black with different infrared characteristics.

(3) Duplicating symbol

Duplicating a symbol means parsing a regular QR symbol and creating the same QR symbol. Since this parsing and symbol creation are difficult to prevent, a unique serial number is added to each symbol. The serial number is verified when the digital signature is authenticated, which enables duplication to be detected.

When two or more regular QR symbols are duplicated, the number of usable duplicates is limited to one because subsequent duplicates are detected by serial number verification during reading. Since the parsing and symbol creation process is costly, it would likely be difficult to obtain a net profit with only one copy. This means that symbol duplication is essentially prevented.

Table 2 summarizes the effects of this proposed method against the three remaining threats.

Table 2 Effects of proposed method against remaining threats

Threat		Digital signature	Public key cryptography	Double encoding	Serial number
Communication	QR symbol				
Eavesdropping	Read secret data	—	○	○	—
Spoofing	Forgery	○	—	—	—
	Duplication	—	—	—	○
	Copy	—	—	○	○
Tampering	Data change	○	—	—	—
Denial		○	—	—	—

III. CONDITIONS FOR IMPLEMENTING SECRET DATA AND DIGITAL SIGNATURE

There are three requirements for QR symbols that contain secret data and a digital signature: compatibility, readability, and separability.

A. *Compatibility*

Compatibility means that, as shown in Fig. 2, the data in the public data area of the QR symbol can be read with existing readers and existing software on smartphones. This is required for upward compatibility; i.e., reading can be done with a reader that does not support symbols containing secret data and a digital signature.

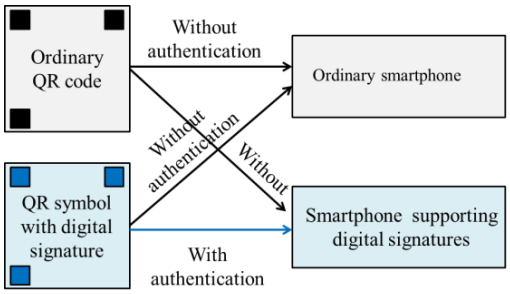

Fig. 2 Compatibility

B. *Readability*

The QR code has an error correction function using the Reed-Solomon (RS) code [1]. This function automatically corrects symbol errors even if there is a reading error within a certain limit | within a certain range. A barcode has a check bit and an error detection function but does not have a correction function. QR symbols that contain secret data and digital signature data require an error correction function for the secret data and digital signature data to ensure readability.

C. *Separability*

The error correction function described above is processed by the smartphone application software without being aware of the function's existence because the data area and error correction data area are separated. If the secret data and digital signature data were mixed in the normal data area, the application software would need to be aware of them, so it is necessary to store them in an area separate from the normal data area.

IV. THREE-REGION QR SYMBOL

In addition to accommodating ordinary public data, secret data and a digital signature must be accommodated in separate independent areas.

The structure of the proposed QR symbol has three areas: a public data area, a secret data area, and a digital signature area. They are implemented by creating two areas in addition to the existing public data area. One is a data area created by area division, and the other is a data area created by double encoding. The three areas are listed in Table 3.

Table 3 Storage area for each data type

Data type	Storage area
Public data	Central sub-cell part
Secret data	Double encode part
Digital signature	Lattice sub-cell part

A. *Area division*

The area division method generates a data storage area while maintaining compatibility with QR codes. It is based on a multi-valued cell method [13] and an area division method [11], which inserts sub-cells at cell boundaries.

A rhombic sub-cell structure is used to accommodate the three types of data: public data, secret data, and digital signature data. Figure 3 shows the symbol structure. Each square area labelled "cell" is a cell in a normal QR code. A central sub-cell is a rhombic region obtained by connecting the centers of the four sides of the outer periphery of a cell; it is used to store public data. The center point of a central sub-cell is the same as the center point of the original cell, which ensures compatibility. A lattice sub-cell is a rhombic region centered on the lattice point where the outer peripheries of four cells intersect; it is used to store digital signature data.

When expanding the data area of the QR code and accommodating the digita signature data in the same area as the public data, there is no separation described in 3.3, and the application software needs to be aware of the existence of the digita signature. On the other hand, by creating a new area by dividing the area, separability is ensured and true compatibility is realized.

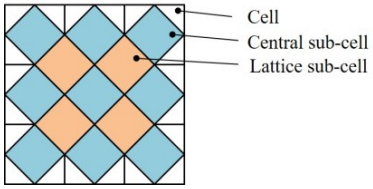

Fig. 3 Configuration of rhombic sub-cell structure

B. *Double encoding*

Double encoding [13] in which the black cell area of the QR symbol is further encoded is used to generate a storage area and copy detection is performed.

The central sub-cell part and the lattice sub-cell part are coded using black and white. In double encoding, the black sub-cells are coded using two more blackish colors.

An example of double encoding using a normal QR code is shown in Figs. 4 and 5. The normal QR code encodes the binarized data (1 and 0) using black and white. In general, binary numbers can be encoded by converting them into two distinguishable states. For example, a bar code is thick and thin, and a Morse code is long and short.

Fig. 4 QR code

Fig. 5 Double-encoded QR symbol

Double encoding uses two dark colors for the black cells of a symbol. Infrared-absorbing black ink (black K) and infrared-transmitting black ink (black CMY) are assumed to be used when the code is printed. Black and blue or black and red are assumed to be used when the code is displayed on a screen. Here, as shown in Fig. 5, encoding is performed with black used for the 1 data and red used for the 0 data.

The QR code consists of a data area for encoding data, a finder pattern (FP) for detecting the presence of a two-dimensional symbol, and a fixed area for checking the alignment patterns and timing patterns, which are used for correcting deformation. Only the black cells in the data area are used for double encoding.

C. *Symbol configuration*

As mentioned above, a QR code has a data area and a fixed area. The fixed area is used for detecting the symbol, correcting distortion, etc. Since normal QR code reading software is based on the assumption of square cells, the cell shape is retained and only the data area is divided.

Figure 6 shows an example QR symbol constructed in accordance with the above policy. The rhombic-shaped sub-cell QR symbol that encodes the central sub-cell and the lattice sub-cell is shown in black and white. Figure 7 shows a symbol in which the dark part of the central sub-cell and the lattice sub-cell are double-encoded in black and red.

We call a symbol that is divided into two regions using rhombic sub-cells a "rhombic sub-cell symbol."

Fig. 6 Rhombic sub-cell QR symbol

Fig. 7 Double-encoded rhombic sub-cell QR symbol

V. STORAGE CAPACITY OF DIGITAL SIGNATURE AREA AND SECRET DATA AREA

A. *Digital signature area*

Here we examine whether the proposed rhombic sub-cell symbol can accommodate digital signature data.

Since the digital signature comprises two sets of 160-bit data, 40 8-bit data code words are required. The preferred error correction rate is 15% or more, the same as for ordinary QR codes.

Table 4 shows the number of data code words that can be stored in each area of a QR symbol for QR code versions 1–4. As shown in the table, version 3 codes and above can store digital signature data along with error correction data code words for a correction rate of about 15%. In version 3, there are 63 code words in the digital signature section (lattice section), so 23 correction code words can be stored (correction rate 17.8%). In version 4 and above, enough error correction data code words can be stored to achieve the maximum correction rate for RS codes (22%).

Table 4 Storage capacity of double-encoded rhombic sub-cell QR symbol

Ver.	Public data area	Digital signature area	Secret data area
	Code word count	Code word count	Code word count
1	26	24	25
2	44	39	41
3	70	63	62
4	100	87	93

B. *Secret data area*

As shown in Table 4, the number of data code words in the secret data area is almost the same as that in the public data area, so the amount of secret data that can be stored is approximately the same as the amount of data that can be stored in the public data area.

VI. PROCESSING ALGORITHM

The process of encoding and decoding a rhombic sub-cell QR symbol with the ECDSA and secret data is shown in Fig. 8.

The printing system downloads software for generating a private key and a public key from a certificate authority and generates them. The generated secret key is kept secret inside the system. The public key and the identity of the issuing entity are sent to the certificate authority to obtain the public key ID. The public key ID has a one-to-one correspondence with the public key.

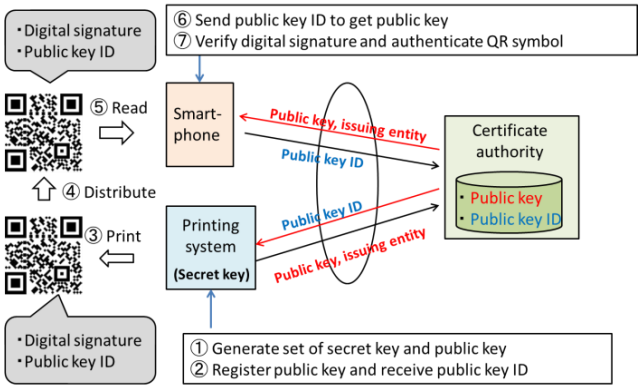

Fig. 8 System configuration

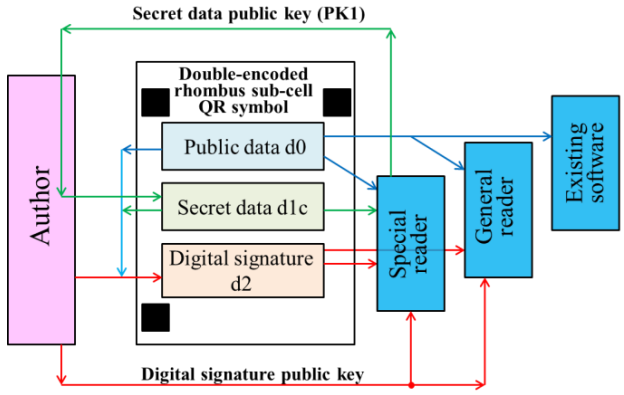

Figure 9 shows the delivery of each type of data as well as that of the public key for the digital signature and secret data.

A. *Data structure*

Table 5 shows the data structure of the rhombic sub-cell QR symbol. The d0 represents public data, which is stored in the normal data part (compatible part), and d1 represents secret data (plain text). The d1c represents secret data obtained by encrypting d1 with the public key. The d2 represents digital signature data for d0 and d1c and is generated by hash function processing and encryption using the secret keys for d0 and d1c. The fd0 and fdc1 represent formatted data in which plain text data d0 and encrypted secret data d1c are compressed in accordance with the specified format for each data type. The fd2 represents formatted digital signature data.

The u0 represents a data code word created using RS code on the basis of fd0 and consists of a data-part data code word (u0,0) and a correction-part data code word (u0,1). Similarly, (uc1,u2) represents a data code word generated on the basis of (fdc1,fd2) and consists of data part (uc1,0,u2,0) and correction part (uc1,1,u2,1).

The pu0 represents the data pattern after pattern mask processing [1] is performed on u0.

Table 5 Data structure

	Public data part (Central sub-cell)		Secret data part (Double encoding)		Digital signature part (Lattice sub-cell)	
	Data section	Correction section	Data section	Correction section	Data section	Correction section
User data	d0		d1			
Encrypted data			d1c		d2 (cd2,0 cd2,1)	
Formatted data	fd0		fdc1		fd2	
Stored data codeword	u0		uc1		u2	
	u0,0	u0,1	uc1,0	uc1,1	u2,0	u2,1
Masked stored data pattern	pu0					
	pu0,0	pu0,1				

B. *Encoding process*

Here, the creation of data code words that correspond one-to-one with each sub-cell for the data contained in each area is called “data encoding,” and the process of encoding these data code words as two-dimensional symbols into optical characteristics is called “symbol encoding.”

Step 1 Preparation of data

The encoding process begins with preparation of public data d0, secret data d1, and digital signature d2 to be stored in the public data section, secret data section, and digital signature section, respectively.

Hash function processing is performed on the data in which public data d0 and encrypted secret data d1c are serially arranged to obtain 160-bit length data. The resulting data is encrypted using the secret key to obtain two 160-bit length data sets, (Cd2,0) and (Cd2,1). These two data sets form the ECDSA digital signature, d2. The public key ID and issuer are set in the padding section.

Step 2 Encoding of public data section

In the coding of the public data part, the central sub-cell is encoded in black and white.

(1) Formatting

Public data d0 is formatted by performing data compression etc. to obtain formatted data fd0.

(2) RS encoding

Data code word u0 is created from fd0 and stored in the public data part. For data code word (u0,0) of the data part, the error correction data code word (u0,1) is created on the basis of the RS code.

(3) Pattern mask processing

Calculation is performed on seven types of mask patterns prepared in advance, and a mask pattern for the compatible part is selected in accordance with a predetermined rule. Pattern mask processing is performed using the selected mask pattern to obtain pu0.

(4) Symbol generation of public data section

The part of the symbol consisting of the central sub-cells containing pu0 is generated. The process in this step is the same as that for generating a normal QR code.

Step 3 Encoding of secret data part

Encoding of secret data is performed by double encoding of the public data section sub-cell and the digital signature section sub-cell. Since the symbol encoding is performed after the digital signature part data is confirmed, only the data encoding of the secret data part is performed in this step.

(1) Encryption

Secret data d1 is encrypted using public key PK1 to obtain d1c. PK1 is a public key made public by the person who receives the secret data.

(2) Formatting, RS coding

Encrypted data d1c is formatted by data compression etc. to obtain formatted data fdc1. Data code word uc1 is created from fdc1 and stored in the secret data part. Error correction data code word (uc1,1) is generated on the basis of the RS code for data code word (uc1,0).

Step 4 Encoding of digital signature part

In the encoding of the digital signature part, the sub-cell of the lattice part is symbol-coded in black and white.

(1) Digital signature creation

A digital signature d2 is created for the merged public data d0 and encrypted secret data d1c (d0d1c).

For the hash function output of d0d1c, d0d1c is encrypted using the secret key of the creator to obtain digital signature data d2.

(2) Formatting, RS coding

Similar to the coding of the public data part in step 2, fd2 is created from d2 and u2 is created from fd2.

(3) Symbol generation for digital signature section

Pattern mask processing is not performed on the digital signature part because the appearance of the same pattern as the FP does not affect detection of the QR symbol. In addition, since the central sub-cell is subjected to pattern mask processing, the position of each lattice sub-cell is accurately calculated. Therefore, partial concentration of the black or white pattern in the lattice sub-cell region and imbalance in the number of black and white sub-cells do not affect sub-cell color identification.

A symbol part is generated consisting of a lattice sub-cell that contains u2. The u2 sub-cell symbol is encoded from the left upper lattice cell to the right lower sub-cell.

The process for this step is the same as that for generating a normal QR code, except for the pattern mask process.

Step 5 Symbol encoding of public and secret data

In the coding of the secret data for the black sub-cell of the public data part generated in step 2 and the black sub-cell of the digital signature part generated in step 4, the sub-cells that make up the black sub-cell are encoded in two black colors. When copy protection is performed for the purpose of preventing forgery, double coding is performed using black K and black CMY. Here, black K is infrared-absorbing black and black CMY is infrared-transmitting black.

(1) Location search for black sub-cells

For the central sub-cell created in step 2 and the lattice sub-cell created in step 4, whether the sub-cell is black or white is determined by following a preset sequence of steps. First, a black sub-cell is selected, and a black sub-cell pointer (Xn,Yn) is created for it, where X and Y are the positions of the sub-cells for which the origin is the upper left part of the QR symbol, and n is the number assigned to the black sub-cells in order. In the black sub-cell search, only the data-code word part is searched; the fixed part is not searched.

(2) Sub-cell layout of black K and black CMY

The data code words are arranged in order of black K and black CMY on the basis of the black sub-cell pointer (Xn,Yn). If the bit of uc1 is 1, black K is placed, and if it is 0, black CMY is placed.

This completes the rhombic sub-cell QR symbol encoding process.

C. Decoding process

Step 1 Image capture

The rhombic sub-cell QR symbol is imaged using white light and infrared light. The white light image data and FP are used to detect the symbol. When it is detected, the image of the rhombic sub-cell QR symbol part is extracted. The infrared light image is used to determine whether a sub-cell is black or white.

Step 2 Public data decoding

(1) Judgment of central sub-cell color

The extracted image is identified as a normal QR code and pu0 is obtained. Next, the pattern mask is released and u0 is obtained.

(2) Decoding of RS code

Error correction processing of the RS code is performed on the basis of u0, and d0 is obtained through fd0.

The process for this step is the same as that for normal QR code decoding.

Step 3 Digital signature decoding

(1) Judgment of lattice sub-cell color

Similar to the process for the central sub-cell, the lattice sub-cell is identified, and uc1 is obtained.

(2) Decoding of RS code

Error correction processing of the RS code is performed on the basis of u2, and d2 is obtained through fd2.

Through this processing, public data d0 and digital signature data d2 are obtained.

Step 4 Secret data decoding

(1) Black sub-cell position search

The black sub-cell is searched for pu0 before the pattern mask release processing in step 2 and u2 and then a black sub-cell pointer (Xn,Yn) is created.

(2) Judgment of sub-cell color

Whether the sub-cell at position (Xn,Yn) in the white light image is black or white at the same position in the infrared light image is determined. By setting 1 for black and 0 for white, u1c is obtained. Since black CMY is an infrared transparent ink, it appears white with infrared light.

(3) Decoding of RS code and decoding of encryption

RS-code error correction processing is performed on the basis of u1c, and d1c is obtained through fdc1. The cipher is decrypted using the secret key of the secret data part, and d1 is obtained.

Through this processing, public data d0, secret data d1, and digital signature data d2 are obtained.

Step 5 Authentication

(1) Acquisition of public key

The public key ID is read from the padding area of formatted data fd0 in the public data part decoded in step 2 and sent to the certificate authority via the network to obtain the public key and issuer.

(2) Authentication process

The acquired public key is used to obtain hash value h0 from digital signature data d2. H0 is obtained from public data d0 and encrypted secret data d1c by performing the processing (hash function processing) performed in step 1 of the encoding process. If h0 and H0 and the issuing subject match, authentication is successful.

VII. Reading Test

The reading of rhombic symbols was tested under the conditions listed in Table 6. The results are plotted in Fig. 10.

Table 6 Reading test conditions

Item		Reading test conditions
Symbols		QR code Ver. 2 Rhombic sub-cell QR symbol Ver. 2
Printing	Printer	Canon (TS8230)
	Paper	KOKUYO (matte paper: 0.15 mm)
Reading	Equipment	SONY (Experia SO-03G)
	Software	DENSO (QR code reader)
	Number of trials	10 each

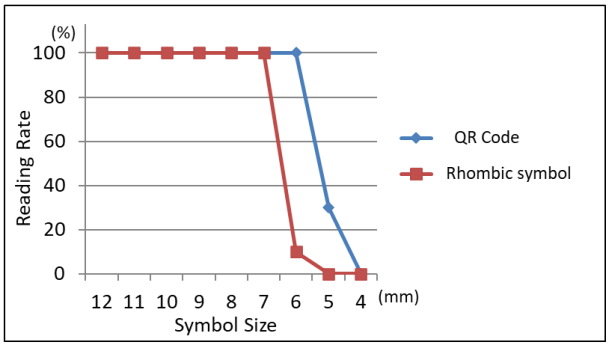

Fig. 10 Reading rate vs. symbol size

Reading software for normal QR code was used for reading the central sub-cell. Reading the sub-cells of the lattice part requires dedicated software, which remains to be implemented. The lattice sub-cell has exactly the same conditions (same shape and size) as the central sub-cell, so the reading characteristics should be the same.

The results show that there was no great difference in discrimination between the QR code and the rhombic sub-cell QR symbol and that the reading limit of the rhombic symbol was slightly large. For version 2 QR code, which was used in the test, a symbol size of 10 to 15 mm is usually used. These results show that rhombic sub-cell QR symbols are sufficiently readable and thus practical.

VIII. Applications

QR codes were first used mostly as data carriers and web references. They are now being used more and more for cashless payments using smartphones as well. Furthermore, applications to prevent counterfeiting are also being considered. Here, we describe applications that could be achieved by adding secret data.

A. Data carrier applications

Data carrier applications include ones for production control and logistics control. With such applications, secret information such as quality information and cost information could be delivered to a specific user. Such applications could even be used for B2C commerce to deliver information to specific customers.

Attaching a rhombic sub-cell symbol to a credit card and accommodating the card number in the secret data area would make it unnecessary to display the card number on the card surface, thereby preventing its disclosure. If a normal QR code is used, the number can easily be read.

Even with cashless payments using a smartphone, security could be improved by storing the main data in the secret data area.

B. Web reference applications

For web reference applications, the public data area could contain a web address that can be referenced by the general public and a secret data area containing a web address that only authorized persons can reference. Those people would be given the secret key needed to read the web address stored in the secret data area. Therefore, as shown in Fig. 11, only a certain group could refer to the secret web address. For example, only people within a company or university could refer to it while everyone else could refer only to the web address stored in the public data area.

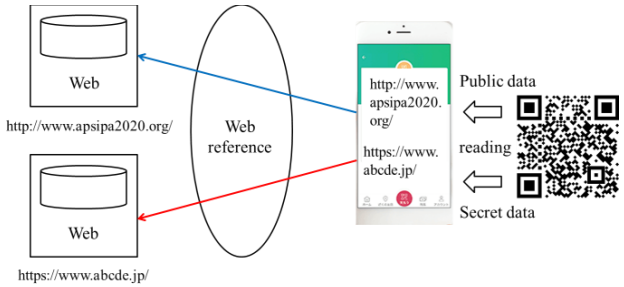

Fig. 11 Web reference by group

C. Counterfeiting prevention applications

Digital signatures are also useful for preventing counterfeiting of securities such as gift certificates and concert tickets and expensive medicines. For securities, it is possible to authenticate the issuer (prevent spoofing) and confirm that the content has not been forged or tampered with. For pharmaceutical products, it is possible to guarantee the contents and prevent counterfeiting. Moreover, a specific

person such as a member of an organization could distribute the secret key and confirm the data stored in the secret data area, which would serve as a more reliable countermeasure against forgery.

IX. SIGNIFICANCE OF COMPATIBILITY

The rhombic symbol was devised to meet the requirement to maintain compatibility with QR codes, and compatibility was demonstrated by the results of the reading test.

This compatibility means that currently used QR codes can be replaced with rhombic sub-cell QR symbols one after another. Although the secret data part and the digital signature part of a rhombic sub-cell QR symbol cannot be read with an existing reader, which means that authentication cannot be performed, the public data can still be read. Once the necessary software is made available, it will be possible to read the secret data part and thus authenticate the creator using the digital signature. The ability of rhombic sub-cell symbols to coexist with ordinary QR codes and their application systems enables their use to be expanded sequentially.

X. CONCLUSION

Our proposed QR symbol is compatible with QR codes, stores secret data with double encoding, and stores a digital signature in a rhombic-shaped sub-cell. Attaching the digital signature to the secret data enables data to be transferred with a high degree of security. The above measures proposed in this paper have made it possible to deal with all of the threats of QR symbols such as reading secret data, forgery, copying, falsification, and denial. Therefore, QR symbols can be applied to a wide range of applications that require high security.

REFERENCES

[1] ISO/IEC 18004:2015 Information technology -- Automatic identification and data capture techniques -- QR Code bar code symbology specification.

[2] Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., Weippl, E.: QR Code Security: A Survey of Attacks and Challenges for Usable Security. In: Int. Conf. Hum. Aspects Inform. Secur. Priv. Trust. Springer, Cham. (2014) 79–90.

[3] Panchal, P., Patil, S.: Android Mobile Security Using Secure Hash Algorithm. Int. J. Comput. Sci. Mob. Comput. 5 (2016) 226–232.

[4] Focardi, R., Luccio, F.L., Wahsheh, H.A.M.: Usable Cryptographic QR Codes. In: IEEE Int. Conf. Ind. Technol., IEEE (2018) 1664–1669.

[5] Warasart, M., Kuacharoen, P.: Paper-based Document Authentication Using Digital Signature and QR Code. In: Int. Conf. Comput. Eng. Technol. (2012).

[6] Razzak, F.: Spamming the Internet of Things: A Possibility and its Probable Solution. Procedia Comput. Sci. 10 (2012) 658–665.

[7] Vaidhyesh, P.S., Mukund, W.N., Shree Varshni, G., Harini, N.: Securing IoT Devices by Generating QR Codes. In: Int. J. Pure Appl. Math. 119 (2018) 13743–13749 .

[8] Wibiyanto, A., Afrianto, I.: QR Code and Transport Layer Security for Licensing Documents Verification. In: IOP Conf. Series: Mater. Sci. Eng. 407 (2018) 012069.

[9] Kashii, Y., Watanabe, Y., Morii, M.: Two-Dimensional Code with Site Authentication Off-Line. Front. Inf. Technol. 11 (2012) 107–112.

[10] Sakina, K.: Digital Signature Type QR Code with Personal Identification Function. IEICE Technical Rep. 117 (2017) 61–66.

[11] Teraura, N, Echizen I, Iwamura K.: Implementation of digital signature on QR symbol by area division using rhombic sub-cells. Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2020. Springer, Cham. (2021) 624–638.

[12] Hara, M.: "Method for producing two-dimensional code reader for reading the two-dimensional code," US patent application 20090323959, by Denso Wave Inc., Patent and Trademark Office, 2009.

[13] Teraura, N., Sakurai, K.: Proposal of multi-value cell structure for high-density two-dimensional codes and evaluation of readability using smartphones. In: 7th International Conference on New Technologies, Mobility and Security (NTMS). Paris (2015) 1‑5.

[14] Teraura, N.: Counterfeit detection by smartphone using double-encoded two-dimensional code. Innovative Mobile and Internet Services in Ubiquitous Computing. IMIS 2017. Advances in Intelligent Systems and Computing 612. Springer, Cham. (2017) 455–466.