MurQRI: Encrypted Multi-Layer QR Codes for Electronic Identity Management

Bonha Koo✉[0000−0001−8299−9193], Taegeun Moon[0000−0002−3477−3509], and Hyoungshick Kim[0000−0002−1605−3866]

Department of Computer Science and Engineering, Sungkyunkwan University
Suwon, South Korea
henahkoo@gmail.com, {taegeun,hyoung}@skku.edu

Abstract. Quick Response (QR) codes are widely used due to their versatility and low deployment cost. However, the existing QR code standard is ineffective for security-critical applications (e.g., electronic identity management) as the stored information can be easily exposed to unauthorized parties. Moreover, it does not provide sufficient storage capacity to employ robust encryption schemes for complex access control and authentication. In this paper, we present a novel approach of employing encrypted multi-layer QR codes, `MurQRI` (pronounced "Mercury"), for secure user authentication and fine-grained access control in various domains (e.g., airport and hospital). `MurQRI` is designed to store up to 45 kilobytes of data and protect the stored information via biometric authentication and encryption. To support fine-grained access control, we employ attribute-based encryption. We also introduce real-world applications where `MurQRI` can be used effectively and discuss possible methods to enhance security.

Keywords: QR Code · Multi-layer QR · Access control · User identification · User authentication.

1 Introduction

A Quick Response (QR) code is a two-dimensional barcode that can encode various types of information. Because the QR code can be used to transfer large data between devices through their display (sender) and camera (receiver), it has been widely used in numerous applications—mobile purchases, print advertisements, and information delivery—to represent an individual's data or authorization ticket. However, the use of QR codes also brings security issues [8, 18]. As anyone can easily read the barcode, it can leak confidential information to unauthorized entities. Moreover, QR codes can be generated for malicious purposes

(e.g., forgery, impersonation) from one's public or easily accessible data. For example, Jaroszewski [16] presented a forgery attack with a maliciously modified QR code. The demonstration involved a crafted QR boarding pass used to access airline lounges and fast-tracks. The attack was successful by simply generating a QR code altering the traveler's name and flight information. This example shows that data embedded in a QR code should be carefully considered for security-critical applications such as electronic identity management.

Several approaches have been proposed to protect QR codes. As explained in Section 6, previous attempts extend from simple secret embedding methods to key encryption [12,13,26,28]. However, existing methods cause inconvenience by requiring large storage space or revealing documented data as plain-text. Further problems of existing methods are high dependency on the server and the absence of fine access control. Ultimately, previous studies integrate conventional QR codes, which are limited to containing trivial data when generated in practical sizes [2]. Overall, there has not been a holistic approach to solving these limitations to establish a reliable electronic identity management scheme.

To overcome such limitations, we propose `MurQRI`, a novel QR code representation scheme to safely store personal data for electronic identification jointly providing fine access-control. Unfortunately, the existing QR code standard cannot directly be used for this purpose because there is no standard protection method for the QR code. It is limited to holding maximum data of 2,953 bytes (in binary mode), which is not sufficient to store an individual's photo or biometric data (see Section 2.1) [15]. As a solution, `MurQRI` expands its data capacity by taking the form of a multi-layer QR and protecting each layer's content with ciphertext-policy attribute-based encryption (CP-ABE). Moreover, `MurQRI` can be further extended with secret hiding techniques to meet the requirements of environments where more complex access control is demanded among multiple parties conveying various privileges to access others' data.

The rest of this paper is organized as follows. Section 2 explains multi-layer QR codes and attribute-based encryption used in `MurQRI`. Section 3 and 4 introduce the proposed `MurQRI` system and describe real-world applications. Section 5 evaluates the effectiveness of biometric input and secret hiding techniques. Section 6 discusses related work. Finally, Section 7 concludes the paper and suggests future work.

2 Background

2.1 Multi-layer QR Code

A Quick Response (QR) code [15] is a two-dimensional barcode that consists of black and white square modules arranged on a grid. The QR code supports 40 versions which differ in size ranging from 21x21 (version 1) to 144x144 (version 40), and 4 different error correction levels: L (7%), M (15%), Q (25%), and H (30%). The amount of data each holds accords to the input mode (e.g., numeric, binary) and error correction level. The QR code can contain diverse forms of

data, including simple texts, URLs, and contacts. Due to its attractive features such as error correction and high-speed scanning, QR codes are widely used in multiple fields today.

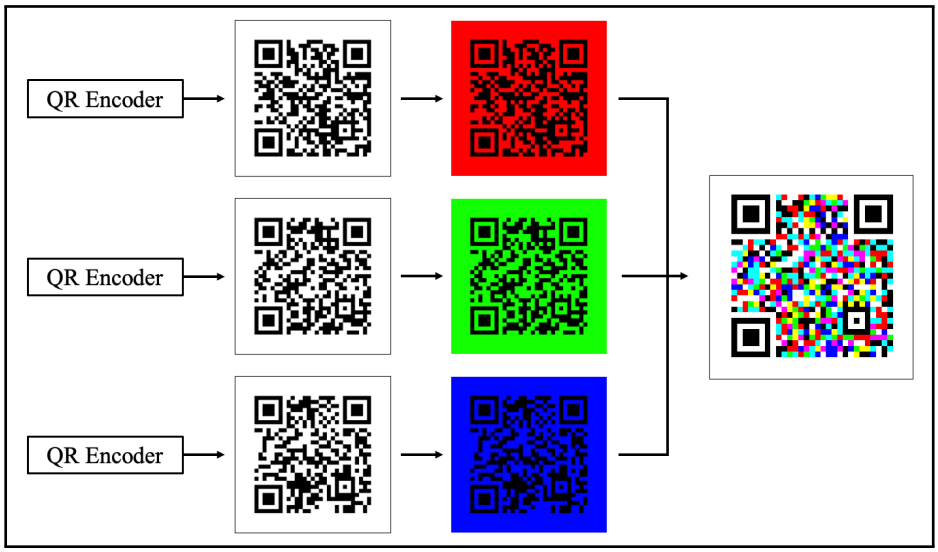

Fig. 1. Example of multi-layer QR code

Multi-layer QR is a relatively new topic introduced to support larger data by expanding the conventional QR code of two dimensions to three. Whereas the standard QR code can store up to 2,953 bytes (in binary mode) [15], multi-layer QR can store much more data because of its extended dimension. Figure 1 shows an example of a 3-layer QR code. Pioneering studies of multi-layer QR [6, 11, 22, 25] suggested utilizing different color channels of the barcode and scanner. Specifically, Dean et al. [11] divided data into three equal-length strings to be embedded into three separate QR codes, allowing the use of a smaller QR version with the same data. Each string was then encoded in the QR format with white modules assigned to red, green, and blue color spaces, respectively. When decoding, layers were separated after color correction, then combined to reconstruct the original string. This scheme observed that any three linearly independent colors are effective in constructing a multi-layer QR code.

However, discoloration of a printed QR code using the RGB channel is yet a problem. To address this issue, Bulan et al. [6] designed an algorithm solving cross-channel color-interference between print-colorant and camera channels. The method they proposed outperformed the preceding method of thresholding for each RGB channel. To develop more practical ways in decoding the multi-layer QR, Noppakaew et al. [25] proposed an algorithm to compute a collection of suitable colors needed to construct n-layered QR codes. They generated a

partition of positive numbers, namely 255, with the length of $\lceil l/3 \rceil$ to construct an l-layered QR code. With the maximum l being 15 in this particular study, the multi-layer QR code can store up to 45 kilobytes, which is about 15 times greater than that of the standard QR code.

2.2 Attribute-Based Encryption

Shamir [28] introduced an identity-based cryptosystem as an extended version of the traditional public key cryptography. Unlike the conventional version, which requires the message to be encrypted with the receiver's public key, identity-based encryption (IBE) can utilize an arbitrary public string (e.g., email address) as the public key. Later, fully functional IBE schemes were devised in [4, 27], which expands "identities" to "descriptive attributes." Ciphertext-policy attribute-based encryption (CP-ABE) takes a further step and links attributes that describe each user to their private key, and embeds the attribute policy within the ciphertext [3, 14]. Therefore, users can decrypt the ciphertext only if their attributes satisfy the access policy.

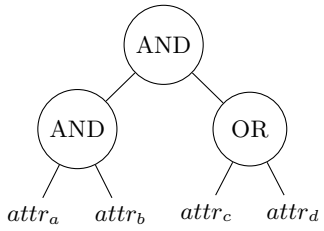

Fig. 2. Access policy tree using AND/OR gates

In CP-ABE, there is a trusted key generator. The trusted party takes charge of setting up the access tree ($\mathbb{A}$) and policy, manages the private master-key, and generates private keys for different parties. Each node in the access tree acts as a threshold gate, and leaf nodes describe attributes (see Figure 2). In addition, although the key generator can be a server for initialization, it is not required for the server to be constantly available after initialization.

The followings are simplified explanations of four algorithms in CP-ABE:

1. `Setup` (λ): The `Setup` algorithm takes the initial security parameter (λ) as input. The outputs are public parameters (p) and the master-key (K_M). p is open to everyone (similar to public key), while K_M should be kept as a secret by the trusted key generator. All entities in one system use the same p for authentication.
2. `KeyGen` (p, K_M, γ): The `KeyGen` algorithm takes p, K_M, and a set of attributes γ as the input. It outputs a secret key K_S for the user with corresponding features.

3. `Encrypt` $(p,\ M,\ \mathbb{A})$: The `Encrypt` algorithm takes p, message to encrypt M, and the access structure $\mathbb{A}$ as input. It outputs a ciphertext C.
4. `Decrypt` $(p,\ K_S,\ C)$: The `Decrypt` algorithm takes p, secret key of a user K_S, and the ciphertext C. It outputs the original message M.

The algorithm reveals M if and only if K_S satisfies γ encrypted in C.

3 Proposed Scheme

`MurQRI` aims to provide an adaptable identification method secure against privacy violation, data misuse, and other security breaches. Figure 3 illustrates the structure of `MurQRI`. `MurQRI` adopts a multi-layer QR code scheme (see Section 2.1) to store larger data organized in categories. In addition, `MurQRI` employs attribute-based encryption (see Section 2.2) to provide stricter authentication and complex access-control. Authorized individuals can hold private attribute keys according to their authority or permission to access the data encoded in users' tag.

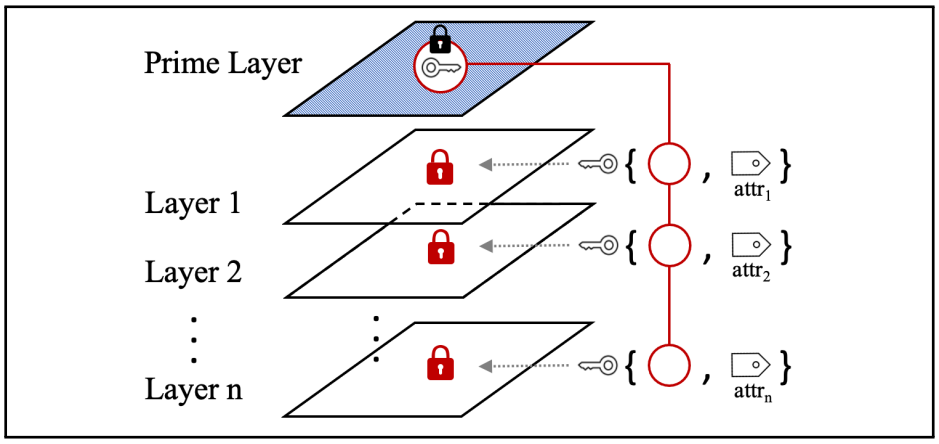

Fig. 3. Overview of `MurQRI`

Figure 4 illustrates encryption and decryption algorithms for a 3-layer `MurQRI`. QR_p, QR_1, and QR_2 are stacked to form the multi-layer QR according to an algorithm devised in Section 2.1. The proposed scheme contains two types of layers with distinct functions: *prime* and *non-prime*. The top-most layer is referred to as *prime layer*. Its sole purpose is to verify the ID holder's authenticity. Therefore, the only data within this layer is an encrypted version of the implicit key (K_i), which can be inferred from the name that this is only used internally. Nevertheless, we discuss encoding additional data in the prime layer in Section 5.2. Encryption and authentication methods for the prime layer differ

upon implementation, described later in this section. *Non-prime layers*, also referred to as "bottom" layers, hold information originally contained in traditional identification documents (see Section 4). Bottom layers are encrypted with two keys, K_i and a layer-specific K_{attr}.

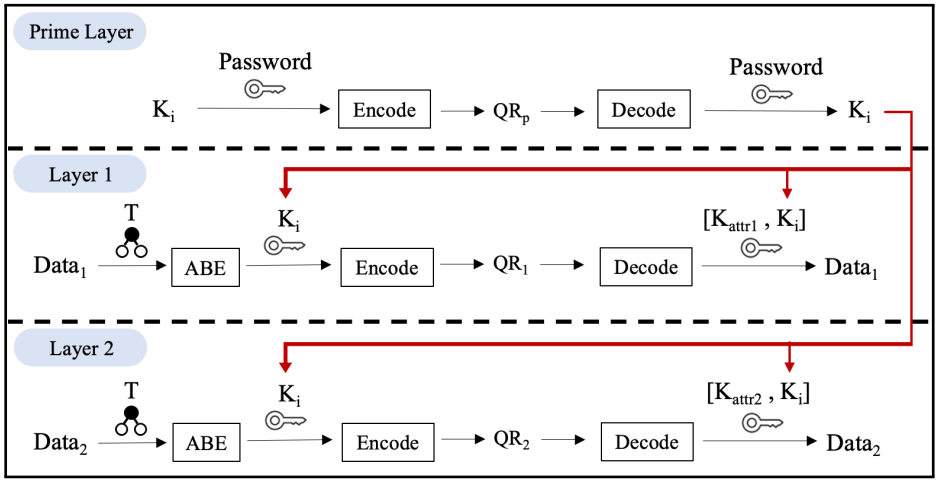

Fig. 4. Example of a 3-layer `MurQRI`

Upon issuance of `MurQRI`, there are multiple ways to encrypt the prime layer. For example, the owner can set a simple passcode (e.g., 4-digit code) or use her biometric data as *Password*. Under this setting, the prime layer encodes K_i, encrypted with a selected *Password*, into a QR code QR_p. In Section 5.1, we discuss how to employ biometric data as an authentication mechanism for `MurQRI`.

The bottom layers deploy ciphertext-policy attribute-based encryption (CP-ABE) for fine-grained access control. To set up non-prime layers, let T and K_{attr} be the access policy tree and private key, respectively. Following the algorithm `Setup` and `KeyGen` in Section 2.2, the trusted key generator sets T and K_{attr}. Then, the ciphertext of plain data is generated according to `Encrypt`. Again, ciphertext for each layer (layer n) is encrypted with K_i, which parties other than the key generator can only obtain by correctly decrypting the prime layer, and then encoded into a QR code QR_n.

This method serves the purpose of both proving the authenticity of the user and providing selective restriction. For example, it is impracticable for a malicious attacker to access data in bottom layers of a stolen tag encrypted with the owner's biometric data, because her biometric input will not match that in the target user's ID. Furthermore, characteristics of CP-ABE convey that users cannot collect private keys and combine them to act as a private key with desired privileges [19]. Along with the infeasibility of a collusion attack, revocation and

delegation of a private key are convenient in this algorithm. Therefore, `MurQRI` implementing CP-ABE can be useful in a large universe with many users and authority levels.

4 Real-world Applications

To demonstrate the practicality of `MurQRI`, we provide two specific real-world use cases.

4.1 `MurQRI` for Electronic Identification in Airports

Because of its convenience, electronic identification is widely used in airports for ePassports and electronic boarding passes [1,29]. Unlike the conventional isolated system, `MurQRI` can serve both functions of an ePassport and a boarding pass to meet real-world efficiency utilizing its security features. The following is a list of information that `MurQRI` could carry in such an environment:

- Default Data: Name, Contact
- Flight Data: Valid flight number, Time, Gate, Seating
- Passport Data: Valid passport number, VISA status
- Biometric Data: Face, Iris, Fingerprint recognition data
- Billing Information

While there are many places this ID could be read, confidential information should not be revealed to those without appropriate permission. For example, the prime layer can be encrypted with a biometric measure (chosen by standard); then, the bottom layers can only be deciphered directly from the owner's correct biometric input. In addition, layer 1 can contain passport information, including confidential data such as her VISA status. Among multiple authorities who can access this ID, airline staff and airport security members should be able to access layer 1, while customer service representatives or cargo handlers should not access or modify this particular information.

4.2 `MurQRI` for Patient Data in Hospitals

Utilizing barcode technology in healthcare is not a new concept. Indeed, advantages in the industry have been proven across multiple years [17, 24]. People are making efforts to put in more data in the barcode, which led to implementing QR codes in line. The main purpose of this is to prevent human-made medical errors and support faster workflow. Additionally, compared to the previous airport scenario, data transmission in a hospital can be more critical.

Consider an example where patient P visits physician H_1 for a health screening, only to find the results be severe cancer. Medical information that could be included in P's ID is as follows:

- Diagnosis and Test Results

- Medication Management: Prescription, Progress logs
- Chemotherapy Instruction: Radiation dose

Regarding medical confidentiality, Physician-Patient privileges are needed to protect P's physical and mental states between P and H_1 [7]. Another physician H_2 cannot access this data even though H_2 has the access level of 'physician.' Additionally, access privileges can be delegated among doctors and hospitals if P chooses to transfer hospitals. `MurQRI` can be useful in this situation as CP-ABE supports easy delegation and revocation of attribute keys. Furthermore, unauthorized staff members are strictly prohibited from modifying drugs or radiation doses of P. By incorporating `MurQRI` in the hospital industry, critical accidents and unintentional data breaches can be prevented.

5 Discussion

In this section, we discuss the effectiveness of biometric data as a key for encrypting K_i and a method of further subdividing a single layer.

5.1 Utilizing Biometric Authentications

The goal of implementing biometric data as a key is to prove the ID owner's authenticity. Face, fingerprint, or iris data can be stored along with biometric engines. For example, templates for each biometric data in [23] are 194 or 322, 800 to 8,000, and 2,348 bytes respectively. Consider the algorithm of Figure 4 with $Password$ as the owner's facial recognition data. Once the reader verifies that a user's face matches the encrypted data, K_i is retrieved. Therefore, bottom layers can be assessed as valid and also be decrypted with appropriate private attribute keys. Real-time comparison of input against the biometric key prevents replay and impersonation attacks. Modifying the prime layer or replacing the QR code is not feasible because attribute policies are defined upon the distributor's issuance. However, as an individual can only generate one key from each biometric feature, security breaches where the biometric data is compromised can be a problem. To prevent this attack, we can embed biometric data with a distributor-generated token, which alters when `MurQRI` is issued. Although generating a fixed key for biometric measures and stability of scanning depends on the environment and selected engine, biometric recognition can further enhance security by linking the owner to the verified document.

5.2 Utilizing Secret Hiding

As `MurQRI` is an electronic identity management scheme, a conventional ID's basic identification functions cannot be ignored. In many cases, revealing the owner's name is not a controversial issue; ID holders do not find it a security breach. Indeed, adding an unencrypted layer for basic identification factors can serve such a function. Even so, there may be cases in which only specific data

within layers should be revealed to the general public. Therefore, we suggest the utilization of secret hiding to disclose data selectively. This scheme can enhance the functionality of an ID and conserve the property of data-categorization.

Secret hiding is a scheme that exploits error correction codewords to conceal secret messages within a cover QR code [20]. QR codewords of a secret message is extracted and embedded into a QR code containing a cover message. Encryption methods or embedding positions differ according to implementation details. Hence, any ordinary decoder can read the cover message, while authorities with prior knowledge of the corresponding decryption method can successfully read the secret message [5, 9, 10].

Returning to the airport scenario in Section 4.1, each layer can embed different public information according to how sensitive the data is. Indeed, the prime layer can select Default Data as the cover message, while ciphertext resulting from encrypting K_i can be the secret. In addition, the layer that includes flight information can select valid flight number, gate, departure time, and seating as public data, while flight validation or reservation codes can be concealed. A recent and most-promising study constructed an algorithm that allows a conventional QR code to hide 10,208 bits of secret message [21]. Adding multiple layers in this scheme provides sufficient space for data in the scenarios mentioned above.

6 Related Work

Previous attempts to secure data within a QR code extend from simple secret embedding methods to key encryption, including employing facial recognition keys. Trujillo et al. [13] introduced an ID authentication system that takes advantage of a (2,2) threshold secret sharing scheme [28]. Two QR code shares, belonging to the distributor and user each, are simultaneously presented and stacked to reveal the secret distinguishable by the human visual system. Yet, this method requires extra storage space to save paired barcodes in order to successfully evaluate authenticity. Similarly, Qryptal [26] suggested IDs including a QR code signed by PKI organization keys and private multi-step pipeline compression. Although this guarantees the authenticity of the document, it still reveals all data to the public in plain-text. The QR code only acts as a tool for authentication while no data is concealed. In contrast, Denso Wave developed Face SQRC [12], which is based on encoding facial recognition data in employee IDs. Although facial recognition data effectively prevents impersonation attacks, the tag can only hold trivial information due to limited data capacity. Overall, existing methods do not address problems of limited encoding space and lack of access control, especially when generated in suitable sizes.

7 Conclusion and Further Work

In this paper, we proposed `MurQRI`, an encryption-based multi-layer QR code scheme for secure electronic identity management. `MurQRI` provides enhanced

security of electronic identification by using encryption and fine-grained access control while providing larger data capacity. The QR code consists of a single prime layer and multiple non-prime layers. The prime layer stores an implicit key, encrypted with a user's password or biometric factor (e.g., fingerprint). Non-prime layers store confidential data encrypted with the implicit key. For the encryption of non-prime layers, we suggest using CP-ABE for fine-grained access control – when a user holds the valid password and private attribute key, the content at non-prime layers can successfully be decrypted. In addition, we suggest a supplementary scheme of secret hiding in QR to enhance the performance of `MurQRI` by providing an option to select public and private data discreetly.

Overall, the proposed scheme allows safer distribution of the ID in public and complex access control. Adopting biometric information as an encryption key assures the integrity and authenticity of the owner. However, any symmetric and asymmetric encryption protocol can be used as well. This flexible scheme could be useful in various applications, such as airports, hospitals, or environments that involve multiple users and different authority properties. For future work, we plan to implement a fully working system of the proposed QR scheme. Given that implementing CP-ABE augments the ciphertext to a substantial size, we also plan to conduct feasibility and usability studies utilizing different cryptographic primitives to find the optimal data size and multi-layering techniques for storing personal data and biometrics.

Acknowledgement

This research was supported by the ICT R&D program (No.2017-0-00545) and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019R1C1C1007118).

References

1. The electronic passport in 2020 and beyond, `https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/passport/electronic-passport-trends`
2. QR code basics: Getting started with QR codes (Jun 2020), `https://www.qr-code-generator.com/qr-code-marketing/qr-codes-basics/`
3. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: 2007 IEEE Symposium on Security and Privacy (SP '07). pp. 321–334 (2007). https://doi.org/10.1109/SP.2007.11
4. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Kilian, J. (ed.) Advances in Cryptology — CRYPTO 2001. pp. 213–229. Springer Berlin Heidelberg, Berlin, Heidelberg (2001)
5. Bui, T.V., Vu, N.K., Nguyen, T.T.P., Echizen, I., Nguyen, T.D.: Robust message hiding for QR code. In: 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. pp. 520–523 (2014). https://doi.org/10.1109/IIH-MSP.2014.135

6. Bulan, O., Blasinski, H., Sharma, G.: Color QR Codes: Increased Capacity Via Per-Channel Data Encoding and Interference Cancellation. In: Color Imaging Conference (2011)
7. California State Legislature: (1965), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=EVID&division=8.&title=&part=&chapter=4.&article=6., division 8. Priviliges Chapter 4. Particular Priviliges Article 6. Physician-Patient Privilege
8. Chambers, B.: How COVID-19 Has Accelerated QR Code Adoption in the UK and EU. Mobileiron.com (Oct 2020), https://www.mobileiron.com/en/blog/how-covid-19-has-accelerated-qr-code-adoption-uk-eu
9. Chiang, Y.J., Lin, P.Y., Wang, R.Z., Chen, Y.H.: Blind QR code steganographic approach based upon error correction capability. KSII Transactions on Internet and Information Systems **7**, 2527–2543 (10 2013). https://doi.org/10.3837/tiis.2013.10.012
10. Chow, Y.W., Susilo, W., Baek, J.: Covert QR Codes: How to Hide in the Crowd, pp. 678–693 (12 2017). https://doi.org/10.1007/978-3-319-72359-4$_4$2
11. Dean, T., Dunn, C.: Quick layered response (QLR) codes (2012)
12. DENSO WAVE: Face authentication SQRC, https://www.denso-wave.com/en/system/qr/product/facesqrc.html
13. Espejel-Trujillo, A., Castillo Camacho, I., Nakano-Miyatake, M., Perez-Meana, H.: Identity document authentication based on VSS and QR codes. Procedia Technology **3**, 241–250 (12 2012). https://doi.org/10.1016/j.protcy.2012.03.026
14. Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded Ciphertext Policy Attribute Based Encryption. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) Automata, Languages and Programming. pp. 579–591. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
15. ISO/IEC 18004:2015(E): Information technology — automatic identification and data capture techniques — QR code bar code symbology specification. Standard, International Organization for Standardization (2015)
16. Jaroszewski, P.: How to get good seats in the security theater? Hacking boarding passes for fun and profit. (May 2016), https://www.defcon.org
17. Khammarnia, M., Kassani, A., Eslahi, M.: The Efficacy of Patients' Wristband Bar-code on Prevention of Medical Errors. Applied Clinical Informatics **6**, 716–727 (12 2015). https://doi.org/10.4338/ACI-2015-06-R-0077
18. Krombholz, K., Fruhwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., Weippl, E.: QR Code Security: A Survey of Attacks and Challenges for Usable Security. In: HCI (2014)
19. Lai, J., Deng, R.H., Li, Y.: Fully Secure Cipertext-Policy Hiding CP-ABE. In: Bao, F., Weng, J. (eds.) Information Security Practice and Experience. pp. 24–39. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
20. Lin, P., Chen, Y., Lu, E.J., Chen, P.: Secret hiding mechanism using QR barcode. In: 2013 International Conference on Signal-Image Technology Internet-Based Systems. pp. 22–25 (2013). https://doi.org/10.1109/SITIS.2013.15
21. Lin, P.Y., Chen, Y.H.: High payload secret hiding technology for QR codes. EURASIP Journal on Image and Video Processing **2017** (12 2017). https://doi.org/10.1186/s13640-016-0155-0
22. Meruga, J., Fountain, C., Kellar, J., Crawford, G., Baride, A., May, S., Cross, W., Hoover, R.: Multi-layered covert QR codes for increased capacity and security **37**, 17–27 (01 2015). https://doi.org/10.1080/1206212X.2015.1061254

23. Neurotechnology: Megamatcher SDK (Nov 2020), https://www.neurotechnology.com/megamatcher-algorithm-tests.html#tests_finger_face_iris
24. Niceware International LLC: Patient Safety with Bar Code and RFID Labeling Identification. White paper (Dec 2006)
25. Noppakaew, P., Khomkuth, S., Sriwilas, S.: Construction of multi-layered QR codes utilizing partitions of positive integers. Journal of Mathematics and Computer Science **18**, 306–313 (05 2018). https://doi.org/10.22436/jmcs.018.03.06
26. Qryptal: The simpler approach to secure and verify documents, https://www.qryptal.com/landingpages/signed-qr-code/
27. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) Advances in Cryptology – EUROCRYPT 2005. pp. 457–473. Springer Berlin Heidelberg, Berlin, Heidelberg (2005)
28. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (Nov 1979). https://doi.org/10.1145/359168.359176, https://doi.org/10.1145/359168.359176
29. SITA: Air Transport IT Insights 2019. SITA https://www.sita.aero/resources/type/surveys-reports/air-transport-it-insights-2019