Journal of KIIT. Vol. 21, No. 4, pp. 125-133, Apr. 30, 2023. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2023.21.4.125

형태보존암호를 이용한 보안 QR 코드 스캔 시스템 구현

최승혁*[1], 조경욱*[2], 한태희*[3], 변연희*[4], 이선영**

Implementation of Secure QR Scan System using Format-Preserving Encryption

Seunghyeok Choi*[1], Kyungwook Cho*[2], Taehui Han*[3], Yeonhui Byeon*[4], and Sun-Young Lee**

2018년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF2018R1D1A1B07047656)

요 약

정보를 전달하는 방법의 하나인 QR 코드는 많은 정보를 담을 수 있지만, Qshing(QR Code Phishing)과 같은 보안 문제가 존재한다. Qshing과 같은 악성 QR 코드로 인한 보안 문제를 예방하기 위해 보안 기능이 추가된 QR 코드가 필요하다. 따라서 본 논문에서는 형태보존암호를 이용한 보안 QR 코드 스캔 시스템을 제안한다. 제안된 시스템에서 QR 코드는 생성과 스캔 과정에서 암·복호화가 진행된다. 암호화된 QR 코드 생성 후, 암호키는 스캔 서버의 DB에 전달되고 QR 코드를 스캔할 때 사용된다. 제안된 시스템에서 QR 코드는 생성 과정에서 암호화되기 때문에 악성 QR 코드로 인한 해킹을 예방하며 공개적으로 노출된 QR 코드에 대해 위변조를 방지하여 무결성과 기밀성을 향상시킨다. 또한 일반 QR 코드 스캔 시스템과 비교하였을 때 유사한 성능을 보인다.

Abstract

QR codes, one of the ways to convey information, can contain a lot of information, but there are security problems such as Qshing(QR Code Phishing). QR codes with added security functions are needed to prevent security problems caused by malicious QR codes such as Qshing. Therefore, In this paper, we propose a secure QR code scanning system using Format-Preserving Encryption. In the proposed system, the QR codes are encrypted and decrypted in the process of generating and scanning. After generating the encrypted QR code, the encryption key is delivered to the database of the scanned server and used to scan the QR code. In the proposed system, QR codes are encrypted in the process of generation, thereby preventing hacking caused by malicious QR codes and preventing the forgery of publicly exposed QR codes to improve integrity and confidentiality. In addtion, it shows similar performance compared to general QR code scanning systems.

Keywords

QR, format preserving encryption, QR scan system, qshing

* 순천향대학교 정보보호학과 학사과정
- ORCID[1]: https://orcid.org/0000-0003-0424-2130
- ORCID[2]: https://orcid.org/0000-0003-3898-4036
- ORCID[3]: https://orcid.org/0000-0002-9719-9292
- ORCID[4]: https://orcid.org/0000-0002-1643-2540
** 순천향대학교 정보보호학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-4686-9436

· Received: Jan. 17, 2023, Revised: Apr. 05, 2023, Accepted: Apr. 08, 2023
· Corresponding Author: Sun-Young Lee
Dept. of Information Security Engineering, Soonchunghyang Univ.,
22, Soonchunhyang-ro, Sinchang-myeon, Asan-si,
Chungcheongnam-do, Korea
Tel: +82-41-530-1357, Email: sunlee@sch.ac.kr

Ⅰ. 서 론

1994년 덴소 웨이브에서 바코드의 한계점을 보완하여 QR 코드가 그림 1과 같이 개발되었다[1].

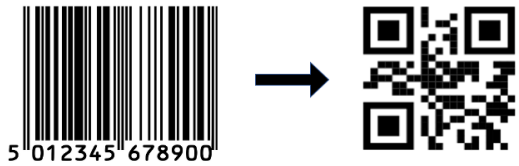

그림 1. 바코드의 진화
Fig. 1. Evolution of the bar code

카메라 스캔 하나로 검색 과정 절차를 줄여 빠르게 검색할 수 있으므로 QR 코드 활용이 증가하여 다양한 분야에서 QR 코드가 활용되고 있다. 예를 들어 버스나 지하철의 광고 홍보물, QR 코드를 통한 결제, QR 정품 인증, 음악 CD, 로또 당첨 여부, 명함, 청첩장 등 다양한 곳에서 QR 코드가 활용된다[2]. QR 코드는 바코드와 달리 이미지, URL, 지도, 명함, 전화번호 등의 데이터를 하나의 코드로 표현할 수 있다. 또한, 코드 일부분이 오염되거나 손상되어도 데이터의 정보를 복원할 수 있다[3].

어느 방향에서나 삽입된 정보에 신속하게 스캔할 수 있으며 2차원으로 정보를 표현하여 바코드와 동일한 정보를 작은 공간에 표현한다. 하지만 QR 코드의 사용이 증가함에 따라 보안 문제 역시 증가하고 있다[4]. QR 코드는 단순히 눈으로 보는 것만으로는 정보 식별이 불가능하므로, 정보가 변형되더라도 즉시 알 수 없어 무결성 검증에 관련하여 피싱 가능성이 크다. 이 때문에 QR 코드 내에 무결성, 인증을 삽입하는 다양한 연구가 진행되었다[1][2][4].

본 논문에서는 QR 코드 정보를 암호화하는 방식[5]과 이를 이용한 스캔 시스템을 통하여 피싱에 대응하는 방법을 제안하였다. 암호화하는 방식에는 AES, DES 등 다양한 알고리즘이 있는데 기존 블록 암호는 암호 값이 블록 크기의 배수가 되기 때문에 정보의 양에 제한이 있는 QR 코드에서 사용하기 어렵다[6].

형태보존암호(Format-preserving encryption)는 암호문이 평문의 길이와 형태를 보존하는 암호로 길이가 일정하게 보존된다. 이는 암호화한 결과가 QR 코드의 이용 가능한 범위를 넘어가지 않으므로 기존 블록 암호 사용의 문제점을 해결할 수 있다. 따라서, 본 논문에서는 정보의 무결성과 기밀성을 보장하기 위해 형태보존암호를 이용하여 암호화하고, 암호화된 QR 코드를 스캔하여 피싱을 방지하는 새로운 QR 스캔 시스템을 제안한다.

2장에서는 QR 코드 및 QR 코드 보안 관련 연구와 본 논문에서 이용한 형태보존암호에 관해 설명하고 3장에서는 제안하는 QR 코드 스캔 시스템의 구성 요소에 관해 설명한다. 4장에선 QR 코드 스캔 시스템을 구현 및 검증하고, 5장에서 일반 스캐너와 제안하는 스캔 시스템의 수행시간을 비교하여 성능을 평가하고 결론을 맺는다.

Ⅱ. 관련 연구

2.1 QR 코드

QR 코드(Quick Response code)는 바코드 형태에서 단점을 보완한 흑백 격자무늬 패턴으로 정보를 나타내며 스캔을 통해 데이터를 빠르게 응답받을 수 있는 매트릭스 형식의 2차원 코드이다[7]. 가로 최대 20자의 숫자 정보만 넣을 수 있는 기존의 바코드와는 달리, 가로, 세로를 활용하여 최대 7,089자의 숫자와 최대 4,296자의 문자, 최대 2,953바이트의 정보를 넣을 수 있다[1]. 또한, URL이나 사진, 지도, 달력, 명함 등을 더불어 영숫자는 물론 한자, 일본어 등의 문자를 포함할 수 있어 다양한 정보를 담을 수 있다[8]. QR 코드는 그림 2와 같이 위치 찾기 심볼(Find pattern), 타이밍 패턴(Timing pattern), 버전 패턴(Version pattern), 얼라이먼트 패턴(Alignment pattern), 포맷 정보(Format information), 데이터(Data)로 구성된다[1].

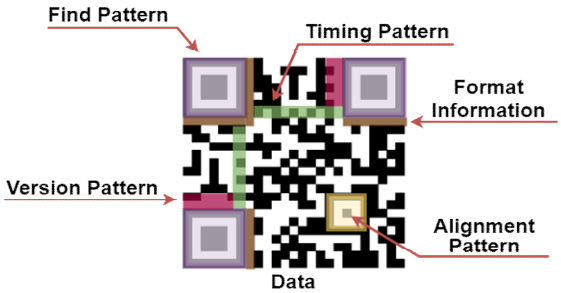

그림 2. QR 코드의 구조
Fig. 2. Structure of QR code

2.2 QR 코드 보안

QR 코드는 어떠한 정보가 담겨 있는지 단순히 눈으로 보는 것만으로는 판별하기 어렵기 때문에 QR 코드 스캐너를 활용하여 정보를 읽는다. QR 코드의 스캔 과정은 QR 코드의 정보를 읽은 뒤 디코딩 과정에서 해독된 정보에 접속하는 방식으로 동작한다. 이러한 과정에서 악성 QR 코드를 구별하는 과정 없이 바로 정보를 디코딩하기 때문에 유해 정보를 담은 악성 QR 코드로 변조된 것을 구별하지 못한다. 이로 인해 QR 코드와 피싱의 합성어인 큐싱(Qshing)이라 하는 개인정보를 탈취하는 문제가 발생하게 된다.

QR 코드의 변조 여부를 확인할 수 없어 발생할 수 있는 보안 위협에 관해 연구되었다[1]. 제안한 기법에서는 공인인증서와 서명 검증을 통한 안전한 URL을 확인하고 기존 PKI(Public Key Infrastructure)를 그대로 활용하지만, 인증서 검증 등으로 인해 사용자 단말의 연산 부담이 있다는 단점이 있다.

클라우드를 기반하여 악성 QR 코드를 탐지하는 시스템에서는 QR 코드를 스캔하게 되면 DB 서버에 저장되어 진 악성 URL 주소와 매칭을 통해 정상 QR 코드로 판단한다[6]. 그렇지만 현재의 시스템은 시그니처 기반 탐지 로직을 사용하기 때문에 알려진 악성코드 URL만 탐지가 가능하다는 단점이 있다.

RFID 시스템의 취약점을 보완하기 위해 Lamport 해시체인으로 일회용 QR 코드를 생성하고 스마트폰 내 애플리케이션을 통해 인증하는 출입 통제 시스템이 제안되었다[2]. 상호 인증에 사용되는 해시값이 매번 변경되어 트래픽 분석과 위치 추적이 불가능하고 값을 유추할 수 없다. 또한, Lamport 해시체인의 해시값을 사용한 결괏값이 노출되어도, 사용할 값을 유추할 수 없어 보안 문제로부터 안전하다.

이처럼 기존 연구에서는 악성 QR 코드를 탐지하여 큐싱을 예방하기 위한 다양한 방식을 제안하였으나 탐지 대상이 URL에 한정되어있거나 알려진 악성코드 URL만 탐지가 가능하다는 등 단점과 한계가 존재했다. 본 논문에서는 기존 연구의 단점을 보완하기 위해 형태보존암호를 이용한 보안 QR 코드 스캔 시스템을 제안하여 위변조된 QR 코드는 식별하지 못하게 하는 것을 목표로 한다.

2.3 형태보존암호

형태보존암호는 1997년 Michael Brightwell 등에 의해 제안되었다[9]. 형태보존암호는 암호문이 평문과 같은 길이와 형태를 갖도록 암호화한다. 기존 블록 암호[10]들과 달리 데이터들의 형태와 길이가 보존된다는 장점이 있다. 형태보존암호는 다양한 알고리즘이 있으며 그 중 FF1과 FF3-1은 Feistel 구조를 기반으로 만들어졌다[11]. FF1과 FF3-1은 AES-128 bit 기반 Feistel 구조를 바탕으로 하는 알고리즘이라는 점에서 유사하지만 각각 다른 구조적 특징을 갖는다. FF1은 10라운드, FF3-1은 8라운드를 사용하는데, 이 각각의 라운드 수 때문에 성능적 측면에서도 다른 특징이 나타난다. FF1은 보호된 포맷 데이터에 대해 더 넓은 범위의 길이를 지원하며, 조정 길이의 유연성을 자랑하는 반면, FF3-1은 FF1에 비해 처리량이 더 높다.

FF1과 FF3-1은 트윅을 사용하는 Feistel 구조를 지닌다. 그림 3은 FF3-1 암호화 알고리즘의 Feistel 구조를 나타낸다. 그림에서 u와 v는 알고리즘 과정에서 분리된 각각의 평문 A_0, B_0길이를, n은 전체 문자 수를, i는 라운드를 의미한다.

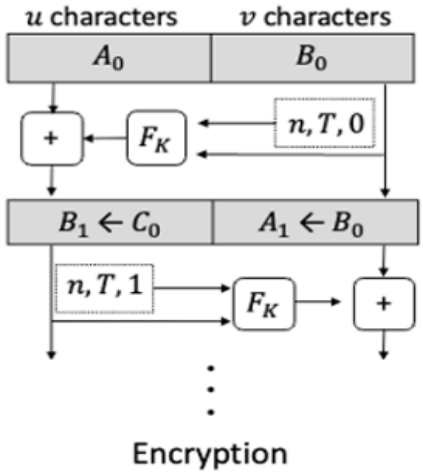

그림 3. FF3-1 암호화의 파이스텔 구조
Fig. 3. Feistel structure of FF3-1 encryption

다음 표 1은 알고리즘 공식에서 사용되는 요소의 정의이다[12].

표 1. FF3-1 필드 정의
Table 1. Field definitions of FF3-1

Field	Description
$CIPH_K(X)$	performing block x encryption using key K
$NUM_{radix}(x)$	converting radix-notation number x into an integer of a decimal number
NUM(x)	converting bit string x to decimal
$STR^m_{radix}(X)$	converting decimal x into a radix number
REV(X)	reversing the numeric string x
PRF(X)	using x as the initial block for CBC encryption mode

FF3-1의 암호화 알고리즘은 키, 트윅, 평문 X를 입력으로 받는다. 트윅의 값은 56비트로 고정되며 암호화 알고리즘의 순서는 다음과 같다. 우선 평문 X를 A와 B 두 부분으로 나누는데, A와 B의 길이는 n의 홀수, 짝수 여부에 따라 달라진다. 트윅은 왼쪽 트윅 T_L과 오른쪽 트윅 T_R로 분리된다. 그 후 라운드 숫자 i가 짝수인지 홀수인지에 따라 m과 W의 값이 결정되며, i, W, B를 사용하여 블록 P를 생성한다. 만들어진 블록 P는 라운드 함수를 거쳐 블록 S를 생성하고, S와 A가 결합되어 동일한 형태와 길이를 보존한 숫자 문자열 C를 생성한다.

Algorithm 1 : FF3-1 Encryption process

1. Let $u = [n/2]; v = n - u$.
2. Let $A = X[1..u]; B = X[u+1..n]$.
3. Let $T_L = T[0..27] \| 0^4$ and
   $T_R = T[32..55] \| T[28..31] \| 0^4$.
4. For i from 0 to 7:
   i. If i is even, let $m = u$ and $W = T_R$, else let $m = v$ and $W = T_L$.
   ii. Let $P = W \oplus [i]^4 \| [NUM_{radix}(REV(B))]^{12}$.
   iii. Let $S = REVB(CIPH_{REVB(K)}REVB(P))$.
   iv. Let $y = NUM(S)$.
   v. Let $c = (NUM_{radix}(REV(A)) + y) \bmod radix^m$.
   vi. Let $C = REV(STR^m_{radix}(c))$.
   vii. Let $A = B$.
   viii. Let $B = C$.
5. Return $A \| B$.

이후 B는 A로, 수정된 $A(C)$는 B로 스왑된다. FF3-1은 이 과정을 8라운드 동안 반복해 값을 생성하며, 암호문은 A와 B의 최종 연산 값이 된다[10].

FF3-1의 복호화 과정은 FF3-1 암호화 과정과 유사하나, 모듈러 덧셈을 이용하는 암호화 과정과 달리 모듈러 뺄셈을 이용한다는 차이점이 있다[10].

Algorithm 2 : FF3-1 Decryption process

1. Let $u = [n/2]; v = n - u$.
2. Let $A = X[1..u]; B = X[u+1..n]$.
3. Let $T_L = T[0..27] \| 0^4$ and
   $T_R = T[32..55] \| T[28..31] \| 0^4$.
4. For i from 7 to 0:
   i. If i is even, let $m = u$ and $W = T_R$, else let $m = v$ and $W = T_L$.
   ii. $P = W \oplus [i]^4 \| [NUM_{radix}(REV(A))]^{12}$.
   iii. Let $S = REVB(CIPH_{REVB(K)}REVB(P))$.
   iv. Let $y = NUM(S)$.
   v. Let $c = (NUM_{radix}(REV(B)) - y) \bmod radix^m$.
   vi. Let $C = REV(STR^m_{radix}(c))$.
   vii. Let $B = A$.
   viii. Let $A = C$.
5. Return $A \| B$.

III. 보안 QR 코드 스캔 시스템 설계 및 구성

제안한 보안 QR 코드 스캔 시스템을 통해 누구나 암호화된 QR 코드를 식별할 수 있다. 제안 시스템으로 생성된 QR 코드는 보안 QR 코드 스캐너로만 복호화할 수 있으므로 위변조되어도 사용자가 큐싱과 같은 악성 QR 코드를 식별할 수 없게 하는 것을 목표로 한다. 또한 QR 코드를 제공하는 사업자가 서로 다른 키를 사용함으로써 사업자만의 무결성 및 기밀성이 보장된 QR 코드를 제공 가능하다. 이는 같은 보안 스캐너여도 복호화하는 키에 따라 스캔 가능 여부가 달라지기 때문에 일반 QR 코드보다 민감한 정보 처리도 가능하다.

QR 코드 스캐너를 통해 사용자가 QR 코드를 스캔하여 디코딩한다는 점은 일반 스캐너와 같지만 암호화키가 저장된 DB가 기반인 스캔 서버를 이용해야 한다는 차이점이 존재한다.

스캔 서버에 암호화된 QR 코드를 보내면 QR 코드에 해당하는 키로 복호화하여 사용자에게 반환한다. 스캔 서버로 요청만 보낼 수 있다면 어느 기기에서도 보안 QR 코드를 이용할 수 있다.

3.1 시스템 설계

본 논문에서는 형태보존암호인 FF3-1 알고리즘을 이용해 데이터를 암호화하여 QR 코드를 생성한다. 암호키는 QR 코드를 생성하는 사업자가 설정한다. 이후 해당하는 암호키로 복호화해야 하므로 암호키는 QR 코드를 생성한 직후 복호화해주는 스캔 서버의 DB에 저장된다. 해당 시스템의 QR 코드 발행과 스캔은 한 서버 내에서 진행한 것으로 키 전달에 대한 무결성이 보장된다. 따라서 그림 4와 같은 시스템을 설계하였다.

3.2 시스템 구성 요소

해당 시스템은 그림 4와 같이 QR 코드 발행, 보안 QR 코드 사용자, 스캔 서버로 구성된다. 각 요소의 역할은 다음과 같다.

QR 코드 발행 : QR 코드로 만들 데이터를 입력하면 사용자가 입력한 키와 트윅 값에 따라 데이터가 암호화되고 암호화된 보안 QR 코드를 생성한다. 또한 보안 QR 코드를 만들 때 사용한 키와 트윅 값은 스캔 서버의 DB로 전달한다.

보안 QR 코드 사용자 : 보안 QR 코드 사용자는 기존과 같이 QR 코드를 스캔한다. 단, 제안한 스캔 서버로 요청을 보낼 수 있는 애플리케이션을 이용해야 한다.

스캔 서버 : QR 코드 발행에서 사용한 키와 트윅 값을 전달받아 DB에 저장한다. 서버는 입력받은 QR 코드에 대해 해당하는 키와 트윅 값으로 복호화하여 사용자에게 반환한다.

IV. 보안 QR 코드 스캔 시스템 구현

4.1 시스템 환경

본 논문에서 설계한 시스템은 모두 파이썬 언어를 기반으로 구현하였다. QR 코드 발행과 스캔 서버는 파이썬 3.8을 이용하며 서버는 Flask, DB는 MySQL을 사용한다.

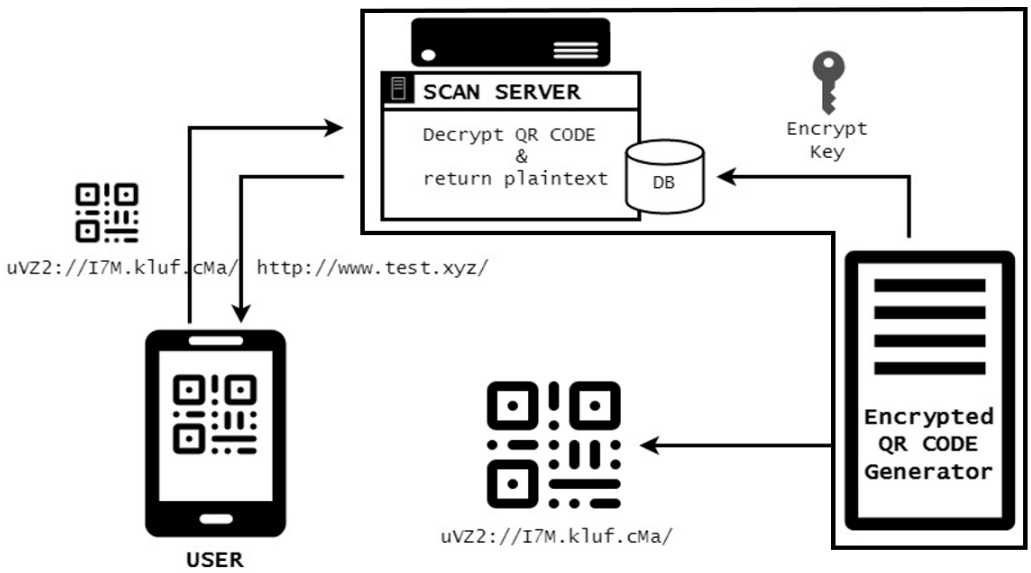

그림 4. 시스템 구성
Fig. 4. Configuration of system

4.2 구현

4.2.1 암호화된 보안 QR 코드 발행 과정

형태보존암호 알고리즘의 암호화를 거쳐 보안 QR 코드를 생성한다. 본 연구의 암·복호화 알고리즘에서는 암호화 대상에 특수문자를 포함하지 않았기 때문에 평문에 포함된 특수문자를 처리 후 암호화를 진행하는 알고리즘을 추가하였다.

암호화된 QR 코드 생성 과정은 그림 5과 같다. 암호화하고자 하는 데이터를 평문으로 한다. 평문에서 특수문자를 제거한다. 이후 사용자가 설정한 키와 트윅 값으로 특수문자가 제거된 평문을 형태보존암호 알고리즘 FF3-1을 이용하여 암호화한다. 이때 암호화에 사용된 키와 트윅 값은 스캔 서버의 DB로 전달되며 암호화 이전에 제거한 특수문자를 암호문에 추가하여 QR 코드를 생성한다.

그림 6은 URL, 휴대전화 번호, 이메일과 같이 다양한 정보를 형태보존암호 알고리즘을 거쳐 암호화된 QR 코드로 만들 수 있다는 것을 보인다. 이처럼 QR 코드에 담을 수 있는 모든 정보는 암호화된 QR 코드로 만들 수 있다.

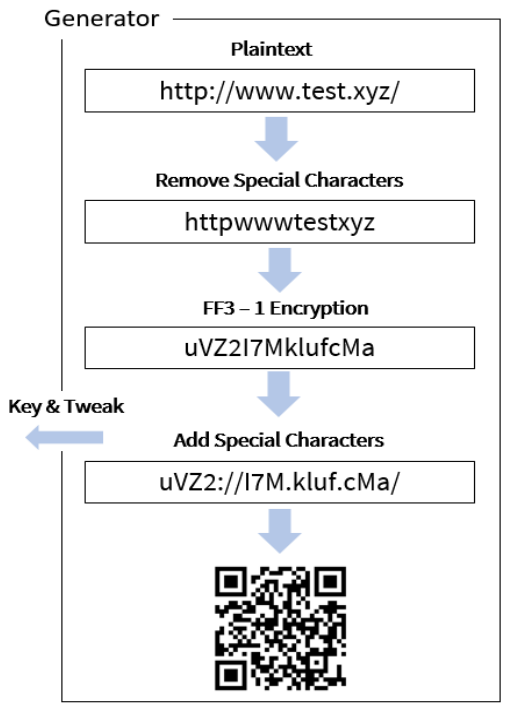

그림 5. 보안 QR 코드 발급 과정
Fig. 5. Secure QR code issuance process

Type	Name Value (URL)	Length	Secured QR Code
None	http://www.text.xyz/	20 bytes	
FPE	51Mr://ieV.pD1A.7cA/		

Type	Name Value (Phone Number)	Length	Secured QR Code
None	tel:+821012345678	15 bytes	
FPE	Dox:+b6w6B93dkMEI		

Type	Name Value (Email)	Length	Secured QR Code
None	MATMSG:TO:logos21.lab@gmail.com;SUB:Hello;BODY:Hi hello;;	58 bytes	
FPE	puSCVh:Dr:NIH4yJV.ifD@oaYxi.Xkz;PRM:eofbs;nuD6:fo hz3Aq;;		

그림 6. 다양한 형태의 정보로 발급된 보안 QR 코드
Fig. 6. Secure QR code with various forms of information

4.2.2 보안 QR 코드 서버 복호화 과정

암호화된 QR 코드 복호화 과정은 그림 7과 같다. 먼저 스캐너는 암호화된 QR 코드를 읽는다. 스캔 서버에서는 읽어 들인 QR 코드의 디코딩을 진행한 후 특수문자를 제거한다. 이후 발행 과정에서 DB로 저장된 키와 트윅 값을 이용해 복호화를 진행한 후 이전에 제거한 특수문자를 평문에 추가하여 사용자에게 반환한다.

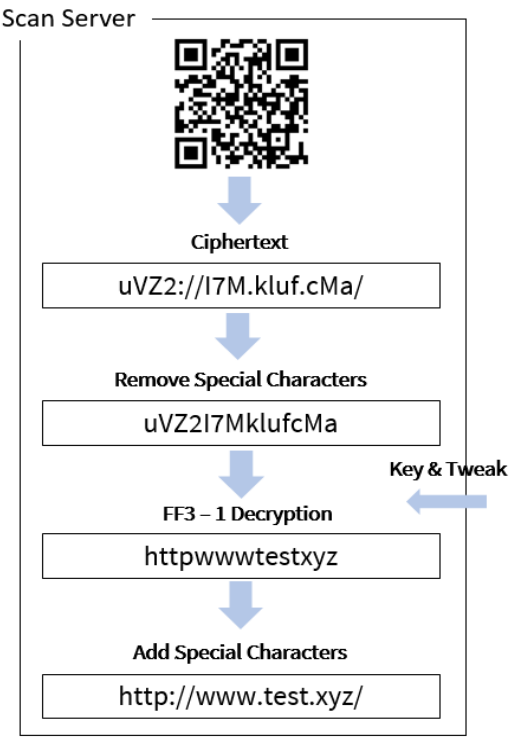

그림 7. 보안 QR 코드 복호화 과정
Fig. 7. Decryption process of secure QR code

V. 실험 결과 및 평가

5.1 실험 결과

5.1.1 정상적인 QR 코드

그림 8은 암호화된 QR 코드를 사용자가 해당 시스템을 통해 스캔한 모습이다. 스캔에 이용된 QR 코드에는 “uVZ2://I7M.kluf.cMa/”라는 암호화된 URL 정보가 담겨 있다. 암호화된 QR 코드를 제안한 시스템으로 스캔하면 “http://www.test.xyz/”라는 정상적으로 복호화된 URL 정보를 나타낸다.

그림 8. 스캐너를 통해 스캔된 보안 QR 코드
Fig. 8. Scanned security QR code via scanner

5.1.2 악성 QR 코드

그림 9는 악성 QR 코드를 해당 시스템을 통해 스캔한 모습이다. 스캔에 이용된 QR 코드는 암호화가 되어있지 않으며 사용자의 로그인을 유도하는 “http://000.000.00.000/accounts/login/?C=” 형태의 피싱 URL 정보를 담고 있다. 해당 스캐너는 키와 트윅 값으로 암호화된 QR 코드를 복호화해서 값을 반환하기 때문에 암호화하지 않은 일반적인 QR 코드나 악성 QR 코드를 스캔할 시 원래의 값을 반환해주지 않는다. 따라서, 큐싱을 예방하고 위변조할 수 없음을 보여준다.

그림 9. 스캐너를 통해 스캔된 악성 QR 코드
Fig. 9. Scanned malicious QR code via scanner

5.2 수행 시간 비교

본 논문에서 제안한 시스템에서의 스캔은 일반 QR 코드 스캔에서 복호화 과정이 추가로 진행된다. 추가한 과정이 성능에 큰 영향을 주는지 확인하기 위해 오버헤드를 측정하였다. 오버헤드는 일반 스캐너에 추가된 복호화 과정에서 발생한다. 따라서 비교 대상이 되는 기존 스캐너의 오버헤드는 0초를 기준으로 한다.

측정에 사용된 데이터는 각각 영어, 숫자, 특수문자가 적절히 조합된 크기가 50 bytes, 200 bytes, 800 bytes, 2950 bytes인 총 4개의 데이터 셋을 사용했으며, 정확한 측정을 위해 스캔을 시작한 후 서버에서 암호문을 디코딩한 시점부터 복호화된 데이터를 반환해주기 전 시점까지의 시간을 측정하였다. 각 데이터 셋당 30번씩 측정을 진행했으며 측정한 값들의 평균을 내어 해당 값을 도출했다. 측정 결과는 그림 10와 같다.

먼저 그림 10에서 보듯이 QR 코드에 담을 수 있는 최대 2953 bytes의 정보를 암호화하는 것이 가능했다. 이는 형태보존암호는 타 블록암호들과 달리 정해진 범위를 전부 사용하며 암호화가 가능하다는 장점을 보인다. 암호화된 QR 코드를 제안한 스캔 서버를 거쳐 스캔했을 때, 일반 스캐너보다 각각 0.0005초, 0.001초, 0.005초, 0.019초의 오버헤드가 발

생하였지만 모두 0.02초 미만의 오버헤드이기 때문에 사용자가 이용하는 데 차이를 느끼기 어렵다.

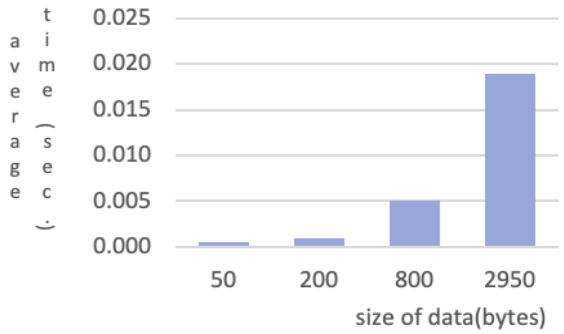

그림 10. 오버헤드 측정 결과
Fig. 10. Results of overhead measurement

Ⅵ. 결 론

QR 코드는 많은 양의 정보를 담을 수 있고, 어디에서나 활용할 수 있다는 장점이 있지만, 활용성이 뛰어난 만큼 안전성이 보장되지 않는다. 또한, 육안으로 보기에는 해당 정보를 판별할 수 없어 위변조 및 큐싱과 같은 보안 문제가 발생한다.

본 논문에서는 위변조 및 큐싱 우려가 있는 QR 코드의 보안 문제를 해결하기 위해 보안 QR 코드 스캔 시스템을 제안하였다.

제안된 시스템은 형태보존암호 알고리즘으로 QR 코드 데이터를 암호화하여 발행한 QR 코드를 이용한다. 사업자가 설정한 키와 트윅 값으로 암호화된 QR 코드를 스캔하면 서버에 저장된 키와 트윅 값으로 해당 QR 코드를 복호화하여 사용자에게 반환한다.

QR 코드 스캔 시 복호화 과정을 필수적으로 진행하기 때문에 암호키를 모르는 공격자에 의한 위변조 공격이 불가능하며, 악성 QR 코드를 스캔하여도 비정상적인 값이 반환되어 악성 QR 코드가 동작하지 않아 보안에서 우수함을 보인다.

제안한 시스템은 기존 연구에서 보였던 단점을 보완하였다. 형태보존암호를 이용해 평문과 암호문의 길이를 유지 할 수 있다는 장점 및 URL 데이터 이외에 모든 데이터에 대한 위변조 QR 식별 불가라는 장점을 보였다. 또한 성능 부분에서 기존의 QR 코드 스캐너와 수행시간을 비교하였을 때 차이가 미미하여 보안 위협에 노출 가능성이 있는 QR 코드에 대해 제안한 보안 QR 코드 스캔 시스템을 통해 사용자의 부담 없이 보안이 강화된 QR 코드를 사용할 수 있다는 것을 증명하였다.

References

[1] H. K. Yang, "A Study of Security Weaknesses of QR Codes and Its Countermeasures", The journal of the Institute of Internet Broadcasting and Communication, Vol. 12, No. 1, pp. 83-89, Feb. 2012.

[2] H. Park, et al., "Improvement of QR Code Access Control System Based on Lamport Hash Chain", International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Springer, Cham, pp. 824-833, Jun. 2019, http://doi.org/10.1007/978-3-030-22263-5_79.

[3] S. J. Choi, M. J. Sim, and H. J. Seo, "The Blockchain Delivery System for Secure Privacy with QR Code and Smart Glasses", Journal of the Korea Institute of Information and Communication Engineering, Vol. 24, No. 5 pp. 630-637, May 2020.

[4] M. S. Ahamed and H. Asiful Mustafa, "A secure QR code system for sharing personal confidential information", 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), IEEE, pp. 1-4, Jul. 2019. https://doi.org/10.1109/IC4ME247184.2019.9036521.

[5] Y. Lee, "Security technology in areas where QR codes are used as intermediaries", Domestic Master's Thesis Pai Chai University Graduate School, 2021.

[6] D. W. Kim, Y. T. Jo, and J. M. Kim, "Cloud-based malware QR Code detection system", Journal of the Korea Institute of Information and Communication Engineering, Vol. 25, No. 9, pp. 1227-1233, Sep. 2021.

[7] S. H. Seo, et al., "QR Code Based Mobile Dual

Transmission OTP System", The Journal of Korea Information and Communications Society, Vol. 38B, No. 5, pp. 377-384, May 2013. http://dx.doi.org/10.7840/kics.2013.38B.5.377.

[8] D. J. Cho and J. S. Koh, "A Study on Method to Improve Recognition Rate of Digital Watermark Using QR Code", The Journal of Korean Institute of Information Technology, Vol. 12, No. 10, pp. 173-179, Oct. 2014.

[9] W. Jang and S. Y. Lee, "Implementation and Performance Evaluation of the Format Preserving Encryption FEA Algorithm", The Journal of Korean Institute of Communications and Information Sciences, Vol. 46, No. 3, pp. 420-429, 2021.

[10] D. Morris, "Recommendation for block cipher modes of operation: methods for format-preserving encryption", NIST Special Publication, Mar. 2016. http://dx.doi.org/10.6028/NIST.SP.800-38G.

[11] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers, "Format-preserving encryption", Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, pp. 295–312, Aug. 2009. https://doi.org/10.1007/978-3-642-05445-7_19.

[12] W. Jang and S. Y. Lee, "A format-preserving encryption FF1, FF3-1 using lightweight block ciphers LEA and, SPECK", Proc. of the 35th Annual ACM Symposium on Applied Computing, pp. 369-375, Mar. 2020. https://doi.org/10.1145/3341105.3373953.

저자소개

최 승 혁 (Seunghyeok Choi)

2021년 3월 ~ 현재 : 순천향대학교 정보보호학과 학사과정
관심분야 : 시스템

조 경 욱 (Kyungwook Cho)

2021년 3월 ~ 현재 : 순천향대학교 정보보호학과 학사과정
관심분야 : 디지털포렌식, 인공지능

한 태 희 (Taehui Han)

2021년 3월 ~ 현재 : 순천향대학교 정보보호학과 학사과정
관심분야 : 인공지능

변 연 희 (Yeonhui Byeon)

2021년 3월 ~ 현재 : 순천향대학교 정보보호학과 학사과정
관심분야 : 리버싱

이 선 영 (Sun-Young Lee)

1993년 2월 : 부경대학교 전자계산학과(이학사)
1995년 2월 : 부경대학교 전자정보공학과(이학석사)
2001년 3월 : 일본도쿄대학 전자정보공학과(공학박사)
2004년 3월 ~ 현재 : 순천향대학교 정보보호학과 교수
관심분야 : 콘텐츠보안, 암호이론, 정보이론, 정보보안