二次元バーコードを利用した暗号の作成

石川県立小松高等学校

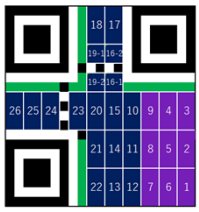
1. 研究の背景と目的

QRコード(*)は、RS(リード・ソロモン)符号という誤りを訂正する機能を持つ符号を使って情報を符号化している。
私たちの研究の目的は、QRコードの誤り訂正機能を利用し、暗号を作成することである。

*QRコードは(株)デンソーウェーブの登録商標です。

2. QRコードについて

・情報を2進数に変換し、決められた順番に配置している。
・1～40の型番があり、型番が大きくなるほどQRコードの1辺のセル数が増加する。
・誤り訂正率にはL,M,Q,Hの4種類がある。
・マスク処理を行い白と黒を反転させることで読み取りを確実にしている。マスクには8種類あり、最適なものが選ばれる。



紫: 情報部分
紺: 符号化部分
緑: 形式情報部分
水: 残余ビット

図1: 1-H型QRコード

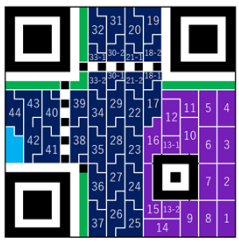


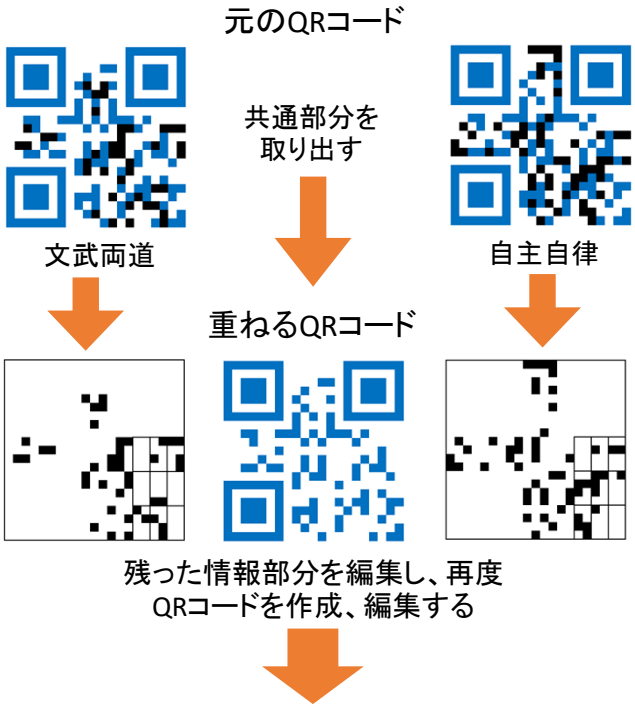
図2: 2-H型QRコード

表1: 誤り訂正レベルの種類と訂正率

誤り訂正レベル	訂正率
L	約7%
M	約15%
Q	約25%
H	約30%

図4:「文武両道」の1-H型QRコード
情報の欠損がみられるが読み取りは可能である。

3. 暗号化の方法



4. 結果

型番1: 新たなQRコードから元のQRコードの情報を読み取れたが、 暗号化したQRコードを作成できない場合があった。
型番2: 新たなQRコードから元のQRコードの情報を読み取れ、すべての場合で暗号化したQRコードを作成できた。しかし、作成したものが読み取れない場合があった。
*暗号化したQRコードの双方と元のQRコードのどちらかがあれば、元のQRコードのもう一方を作成することができた。

5. 考察

・型番1では、誤り訂正可能数の不足から暗号化したQRコードを作成できなかったと考えられる。
・型番2では、誤りを含ませる位置やマスクの問題で作成したものが読み取れなかったと考えられる。
・この暗号は2つの情報から2つの暗号と1つの共通鍵を作成するため、総情報量の増加をはじめの150%に抑えることができる。そのため、容量を抑えて暗号化したい場合に活用できると考えられる。

6. 結論

上記の方法でQRコードを利用した暗号は作成できる。しかし、作成に条件があり、任意の情報では作成できない場合がある。

7. 参考文献

・https://www.taf.or.jp/files/items/566/File/030.pdf
・先名健一著　例題で学ぶ符号理論入門(森北出版)
・池田和興著　例題が語る符号理論-BCH符号・RS符号・QRコード(共立出版)

石川県立小松高等学校　02

二次元バーコードを利用した暗号の作成

抄録

本研究では、QR コードに用いられている誤り訂正技術を利用して QR コードを暗号化した。作成した結果、QR コードの暗号化には成功したが、読み取りやすさや暗号化の確実性にはまだ問題があることが分かった。

１．研究の背景と目的

QR コード*には、RS 符号と呼ばれる誤り訂正符号が搭載されている。本研究の目的は、この技術を利用し暗号化された 2 つの QR コードに、共通鍵となる QR コードを重ねることで復号できる QR コードを作成することである。　*QR コードは(株)デンソーウェーブの登録商標です。

２．方法

型番 1(21×21)で 2 種類の同じ文字数の情報を含んだ QR コードを作成する。これを QR(A)，QR(B)とする。QR(A)，QR(B)の情報のうち、両方に含まれる部分を「重ねる QR コード」QR(*)とし、残りの部分を利用して新たな情報部分を作成し、QR コード QR(x)，QR(y)を作る。そして QR(x)，QR(y)それぞれと QR(*)を重ねることで新たに現れる QR コード QR(α)と QR(β)が読み取れるかどうか、またそれらの情報がそれぞれ QR(A)，QR(B)と一致するかを調査した。同様の手順で型番 2(25×25)の QR コードも作成した。

３．結果

型番 1 では、一部の情報で QR(x)と QR(y)，QR(α)，QR(β)を作成し、読み取ることができた。QR(α)と QR(β)の情報はそれぞれ QR(A)，QR(B)の情報と一致した。型番 2 ではどのような場合でも QR(α)，QR(β)を作成できたが、型番 1 の場合よりも読み取りに時間がかかった。また、作成した QR コードのうち QR(x)，QR(y)の双方と QR(A)または QR(B)があればもう一方の QR コードを作成できた。

図 1: 左から、「文武両道」と「自主自律」の情報から作成した QR(x)，QR(y)，QR(*)。

４．考察

型番 1 では、誤り訂正可能数の関係により、QR(α)と QR(β)が正しく読み取れる QR(x)，QR(y)が作成できない場合があった。一方、型番 2 では読み取りに時間がかかったが、どのような情報でも正しく読み取り可能な QR(α)，QR(β)を作成できた。そのため、適切な型番を選択することで確実に暗号を作成することができるが、型番が大きくなると読み取りが難しくなっていくと考えられる。

５．結論と今後の課題

QR コードを利用した暗号化は可能であった。しかし、型番によっては暗号化できない場合があることや、読み取りに時間がかかることなどの問題がある。今後は読み取り精度の改善や、QR(x)，QR(y)の情報を任意のものに設定できるような方法を考えていきたい。

６．参考文献

・https://www.taf.or.jp/files/items/566/File/030.pdf
・先名健一著　例題で学ぶ符号理論入門(森北出版)
・池田和興著　例題が語る符号理論 ―BCH 符号・RS 符号・QR コード(共立出版)

７．キーワード

QR コード　誤り訂正符号