K-007

電子署名を有するカラー菱形サブセル QR シンボルの検討
A Study on Color Rhombic Subcell QR Symbol with Digital Signature

寺浦 信之[†1]　越前 功[†2]　岩村　恵市[†3]
Nobuyuki Teraura　Isao Echizen　Keiichi Iwamura

1. はじめに

1.1 電子署名によるセキュリティの実現

現在の QR コード[1]は、誰でもが簡単に作成することが可能であり、また誰でもがスマホを用いてデータを読取ることが可能である。作成が容易なので、なりすましや偽造が容易に実行可能である。最低限のセキュリティとして作成者が明確であることがある。

作成者の認証のために、QR シンボルに電子署名を実装することが提案されている。本論文では、新たな多色化シンボル構成を検討し、公開データに電子署名を付して偽造、改ざん防止を行うことを提案する。

ここで、ISO/IEC の国際標準[1]に合致する二次元シンボルを QR コードと呼び、互換性はあるが異なる仕様部分がある二次元シンボルを QR シンボルと呼ぶ。

1.2 既存の研究

1.2.1 電子署名の実装

QR シンボルに電子署名を実装する提案が種々の目的でなされている[2] - [4]。また、実際に ECDSA を通常のデータ部に実装する事例がある[5] - [8]。これらは、通常の QR コードをそのまま用い、データ部にアプリケーションに必要なデータに加えて、ECDSA のデータを併記するものである。これに対して、通常のデータ部とは別個のデータ領域を作り出し、アプリケーションのデータとは分離して電子署名を実装する提案がなされている[9] [10] 。 [9]は、QR シンボルのデータ領域の未使用領域(埋め草領域）に RSA 電子署名を実装している。[10]は、ECDSA 電子署名を QR シンボルの誤り訂正データ領域に XOR して埋め込んでいる。

一方、著者等は、菱形サブセルを用いて電子署名をシンボルに埋め込む提案をしている[11] 。

1.2.2 データ記憶空間の拡大

QR コード等の二次元シンボルのデータ記憶容量を拡大する手法として、二次元シンボルを構成する基本単位であるセルを多色化し、多値化する手法が提案されている[12]-[17]。また、セルを複数のサブセルに分割し、サブセルを符号化の単位とする手法が提案されている[18]。

1.3 既存研究の課題

[11]では、菱形サブセルを用いて ECDSA を実装し、電子署名実装の課題を解決している。しかし、データ量の少ない ECDSA の電子署名を用いても、小さなバージョンの菱形サブセル QR シンボルに収容することは困難である。そこで、電子署名を収容する領域を多色化し、収容データ容量を拡大して、小さなバージョンのシンボルにおいても収容可能とする。

2. 電子署名実装の条件

電子署名を収容する QR シンボルに必要とされる要件について述べる。

2.1 互換性

互換性とは、図 1 に示すように、既存の読取り装置やスマホの既存のソフトで、QR シンボルの公開データ領域のデータを読取り可能であることである。この互換性は電子署名を収容するシンボルに非対応の読取り装置で読取りを可能とする上位互換の要件である。

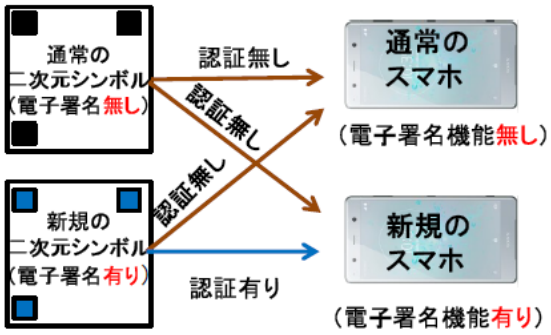


図 1　互換性

2.2 読取り性

QR コードには、RS 符号を用いた誤り訂正機能が具備されている[1]。この機能は一定限度内の読取り誤りがあっても、自動的に訂正する機能である。バーコードにはチェックビットがあり、誤り検出機能を有するが、訂正機能を有しない。電子署名データを収容する QR シンボルにおいても、読み取り性を確保するために、電子署名データの誤り訂正機能が必要である。

2.3 分離性

上記の誤り訂正機能は、スマホのアプリケーションソフトがその存在を意識せずに処理がなされている。これはデータ領域と誤り訂正データ領域が分離されており、システム側で処理されているからである。電子署名データも、通常のデータ領域に混在されていればアプリケーションソフトが意識する必要があるので、通常のデータ領域とは分離された領域に収容される必要がある。

†1 テララコード研究所、 Terrara Code Research Institute
†2 情報学研究所、 National Institute of Informatics
†3 東京理科大学、 Tokyo University of Science

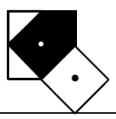
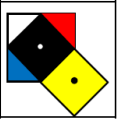
3. 新しいデータ空間の創造

前節で述べたように、互換性を実現するためには、電子署名データは、ユーザデータとは別の領域に記憶される必要がある。

別の記憶領域を作り出す方式としては、符号化の基本単位であるセルそのものの多値化手法[16] -[18]とセル間へサブセルを挿入する領域分割手法[11]がある。これらを表 1 に示す。

次に、これらの多値化手法について概説する。

表 1　互換性を保つデータ空間の生成方式

方式	セルの多値化			領域分割	
手法	多色化 [16]	セル分割多色化 [17]	セル分割 [18]	白黒 [11]	多色化
セル及びサブセル形式					

3.1 セルの多値化

白または黒で表現されるセルでは 1 ビットを符号化している。それに対して、複数ビットを符号化するのがセルの多値化である。セルの多値化には、多色化と多領域化がある。

3.1.1 多色化

多色化は、通常のシンボルが黒と白の二つの色で 1 ビットを符号化しているのに対して、例えば、白と黒に黄と赤を加えた 4 色を用いると 2 ビットを符号化できる。さらに、8 色では 3 ビットを符号化する[16]。 8 色で QR シンボルを構成した例を図 2 に示す。

但し、単純な多色化では、次節で述べるように、互換性を保つことは困難である。

図 2　多色化セルによる QR シンボル

3.1.2 セル分割

セル分割は、表 1 に示すように、セルを複数のサブセルに分割し、サブセルを符号化の単位として符号化する[18]。9 個のサブセルに分割し、それぞれのサブセルを独立して白と黒で符号化すると 9 ビットを符号化できる。

但し、全てのサブセルを独立して符号化すると互換性を保つことは困難であり、特別な対応が必要である。

3.1.3 セル分割多色化

多色化とセル分割を同時に用いる提案もなされている[17] 。セルを 9 個のサブセルに分割し、それぞれのサブセルに独立して 8 色で符号化すると 27 ビットを符号化できる。

この場合も、独立した配色では互換性を保つことは困難であり、サブセルへの配色に制限を加えることが必要となる。

3.2 領域分割

セルの多値化はセル内部の対応である。セルの多色化はセルそのものの配色であり、セル分割はセル自体を分割し、他のセルの領域とは独立している。それに対して、領域分割は表 1 に示すように、セルの枠を超えて、シンボルの領域を分割する。詳細は、第 5 節で述べる。

4. 互換性を考慮したカラー符号化

4.1 セルの符号化

図 2 に示した多色化セルの QR シンボルは、表 2 に示す符号化テーブルに基づいて符号化されている。表 2 に示す 8 色が用いられており、白グループの 4 色と黒グループの 4 色に分けられている。QR コードとの互換性を保つために、例えば QR コードで白セルに対応させる場合には白グループの色から、符号化データに対応する色を割り当てている。白グループ色は輝度が高く、黒グループ色は低い。また、白グループの中で輝度が最小の緑と黒グループの中で輝度が最大の桃では輝度が大きく開いており、この配色により互換性を補完している。

表 2　符号化テーブル（8 色）

色群	色	RGB成分 R	G	B	輝度	符号化データ
白グループ	白	255	255	255	1	00
	黄	255	255	0	0.93	01
	水	0	255	255	0.79	10
	緑	0	255	0	0.72	11
黒グループ	桃	255	0	255	0.29	00
	赤	255	0	0	0.21	01
	青	0	0	255	0.07	10
	黒	0	0	0	0	11

4.2 セルの構造

図 2 に示す多色化セルによる QR シンボルでは、互換性が安定しない。その原因は、色のばらつきである。プリンタによる色のばらつきや色の経年変化があり、互換性の維持は困難である。

図 2 のシンボルをパソコン上で生成し、それを画面上に表示する場合は、表示色は一定程度再現され、既存のリーダで読取れる場合がある。一方、このシンボルを紙に印刷し、それをスマホで読取る場合には多くの場合読み取ることができない。印刷時には RGB から CMYK のインクの表現に変換され、さらにスマホによって読み取られるときに RGB 値に変換される。これらの処理毎に色空間が縮退し、明度差が小さくなり、既存の読取り装置では読めなくなる。

そこで、既存の QR コードのリーダがセル中央をサンプリングしていることに着目して、サンプリング部分を白または黒とすることで安定した互換性を実現可能である。これを実現するために、図 3 に示すように、セルを 9 分割し、中央部と周辺部に分割する。

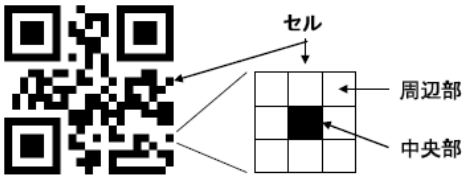


図 3　セルの分割

中央部は白または黒で互換データを符号化し、周辺部を表 2 の符号化テーブルに基づいて符号化を行う。この場合、中央部（互換データ）に 1 ビット、周辺部（追加データ）に 2 ビットを符号化する。これにより、安定した互換性を実現することができる。このセル分割多色化を行った QR シンボルを図 4 に示す。

図 4　セル分割を行った互換性多色化 QR シンボル

5. 菱形サブセル QR シンボル

5.1 菱形サブセル

互換データ及び電子署名データの二つのデータを収容するシンボルとして、菱形サブセルを用いたシンボルを検討した[11]。このシンボルのサブセル構成を図 5 に示す。図 5 で、セルと記載されている正方形の領域は、通常の QR コードにおけるセルである。中央部サブセルは、セルの外周の 4 辺の中央部を結んで得られる菱形領域であり、公開データを収容する。中央部サブセルの中心点は、元のセルの中心点と同一であり、互換性を実現する。格子部サブセルは、セルの外周が交差する格子点を中心とする菱形領域であり、電子署名データを収容する。

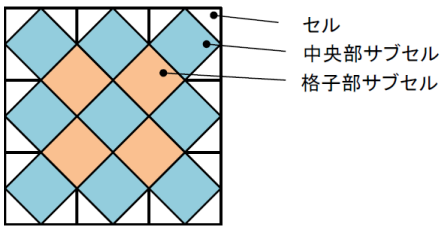


図 5 菱形サブセルの構成

5.2 シンボルの構成

QR コードでは、データを符号化し、収容するデータ領域と二次元シンボルの存在を発見するファインダーパターン、変形を補正するためのアライメントパターンやタイミングパターンの固定領域から成る。固定領域はシンボルの存在検出や歪み補正などに用いられ、通常の QR コードの読取りソフトは正方形のセルを前提としているので、互換性を維持するためにセル形状を保持し、データ領域のみ領域分割を行う。

上記の方針で QR シンボルを構成した例を図 6 に示す。菱形サブセルを用いて 2 領域分割を行った QR シンボルを以下では菱形サブセル QR シンボルと呼ぶ。

図 6 菱形サブセル QR シンボル

6. カラー菱形サブセル QR シンボル

前節では、サブセルを白と黒で符号化する菱形サブセル QR シンボルについて述べた。本節では、菱形サブセル QR シンボルにおいて、電子署名を収容する格子サブセルを多色化し、大容量化することを検討する。

6.1 格子部サブセルのカラー符号化

菱形サブセル QR シンボルの中央部サブセルは、QR コードとの互換データ（公開データ）を保持している。そこで、互換性の維持の観点から、中央部サブセルは白と黒の 2 色で符号化する。そして、互換性とは関係しない格子部サブセルを多色化する。ここでは、多色化は白と黒に赤と青を加えた 4 色を用いる場合について説明する。

160 ビットの ECDSA の電子署名では、電子署名データは 320 ビットとなる。また、この電子署名データに対する RS 符号の誤り訂正データを加えたデータを格子部サブセルに収容する。これらのデータを 2 ビットずつに分割し、表 3 に示す符号化テーブルで定義した色を選択し、特定の格子部サブセルに配色する。例えば、2 ビットのデータが 00 であれば白であり、10 であれば青となる。このように配色したサブセル構成の例を図 7 に示す。中央部サブセルは、白と黒の 2 色で符号化され、格子部サブセルは白赤青と黒の 4 色で符号化されている。

表 3　符号化テーブル（4 色）

色	RGB成分		符号化データ
	R	B	
白	○	○	00
赤	○	×	01
青	×	○	10
黒	×	×	11

図 7　カラー菱形サブセル構成の例

これらをカラー菱形サブセル QR シンボルとして構成した例を図 8 に示す。

図 8　カラー菱形サブセル QR シンボル

7. カラーセル QR とカラー菱形セル QR の比較

この節では、第 4 節で述べたカラーセル QR シンボルと前節で述べたカラー菱形サブセル QR シンボルの比較を行う。

7.1 ロバストネス

カラーセル QR シンボルとカラー菱形サブセル QR シンボルのシンボルとしての性能の第 1 の差異は、ロバストネスにある。二次元シンボルのロバストネスの構成要因を表 4 に示す。

表 4　ロバストネスの構成要因

分類		要因
アナログ	シンボル形状	セルの形状
		セルの配置
	印刷	セルの大きさ
		セルの印刷精度（DPI）
		セルの明度比（PCS）
		バージョンの小型化
アナログ／ディジタル	データ圧縮	データ量縮減によるバージョンの小型化
	マターンマスク	セルの白黒配置によるセル位置補正
ディジタル	誤り訂正	データ部のRS符号
		管理部のBNC符号

表 4 の中で、両シンボルの差異は、セル（サブセル）の大きさにある。次に、セルの大きさとロバストネスの関係について検討する。

7.1.1 セル（サブセル）の大きさ

QR シンボルを読取る時、シンボル画像のセル画素のサンプリングを行う。セル内部のサンプリング値は、周囲のセルからの影響を受ける。それは、撮像時のピンボケ、手振れ、平均化処理等が原因である。ここで平均化処理に着目する。スマホなどでは、撮像画像の画面表示を行い、その表示された QR シンボルの画像に対して識別を行っている。画像表示にあたって、画像の圧縮処理が行われており、その際に画素の平均化処理がなされて、セルの周辺領域には、セルの周囲のセル色の影響が及ぶ。また、ピンボケや手振れなどでも、同様に周囲のセル色の影響がセル周辺部に及ぶ。これらの状態を図 9 に示す。これらの影響の及ぶ領域を浸潤領域と呼ぶ。そこで、周辺部セル色の影響が最も小さい位置は、セルの中心である。サンプリング時に、セルの中心位置を計算し、その位置の画素データをサンプリングデータとする。しかし、QR シンボル画像の歪みなどで、セル中心の推定位置は真の中心位置から離れ、セル中心位置の周りに分布する。この推定中心位置の分布する領域をサンプリング領域と呼ぶ。また、サンプリング領域と浸潤領域の中間領域をバッファー領域と呼ぶ。

通常の QR コードでは、セルサイズが大きく、バッファー領域が十分確保できているので、正しいセル色のサンプリングを行うことが可能である。しかし、シンボルの物理的サイズが小さくなり、またはバージョンが大きくなり、セルが小さくなると、図 10 に示すように、バッファー領域は縮減し、消失する限界セルサイズとなる。限界セルサイズよりも小さなセルでは正しいサンプリングは困難となる。

ここで、浸潤長 δ はセルの大きさに依存せず、撮像する環境によって定まり、一定と考えられる。そこで、セルが大きいほど安定した識別が可能である。すなわち、ロバストネスが大きい。

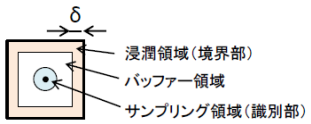


図 9　セルの領域

図 10　限界セル

7.1.2 セル（サブセル）の大きさ

カラーセル QR シンボルのセルは、互換性を保つために、中央部のサブセルが白または黒となっており、カラー符号化色とは異なっている。そこで、カラーセル QR シンボルでは、そのサンプリング位置は中央部サブセルではなく、周辺部のサブセルの中心位置をサンプリングする。これは、周辺セルや中央部サブセルからの距離が等しく、影響が一番小さいからである。サンプリング点は図 11 及び図 12 に示す中間点型と角点型に分類できる。中間点型は、周辺部サブセルの中で、中間にあるサブセルであり、角点型は角にあるサブセルである。中間点型は、その上下または左右が同じ色のサブセルであり、その左右または上下が異なる色の可能性がある。角点型は、上下及び左右の 2 つが同じ色であり、また 2 つが異なる色の可能性がある。ここでの検討では、上下左右のサブセルのみが相互に影響があり、斜めのサブセルは影響しないと仮定している。

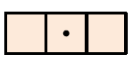


図 11　中間点型

図 12　角点型

これらでは、サンプリング対象のサブセルに接する半数がサブセルの一辺の半分の長さで他の周辺のセルまたは中央サブセルと接しており、残りの半分がその 3 倍の長さで接している。

そこで、サンプリング点から境界までの実効的な評価基準として面積を用いることとする。この場合、中間点型も角点型もセル面積の 1/3 の面積となる。一方、菱形サブセルの面積はセル面積の 1/2 の面積である。これから、菱形サブセル QR シンボルのほうが、セルの大きさによるロバストネスが大きいと言える。

7.2 データ容量

次に、データ容量の比較を行う。カラーセル QR シンボルでは、8 色を用いて符号化した場合には、互換部データとして中央部サブセルに 1 ビットが符号化され、周辺部に 2 ビットが符号化される。周辺部が 2 ビットであるのは、表 2 の符号化テーブルに示すように、互換部を補完するために、中央部が黒である場合には周辺部は黒グループの 4 色を用いて符号化しているからである。

カラー菱形サブセル QR シンボルでは、8 色を用いて符号化した場合には、互換部データとして中央部サブセルに 1 ビットが符号化される。そして、格子部サブセルには 3 ビットが符号化される。格子部サブセルは中央部には影響を与えないセルの 4 端に配置されており、中央部サブセルと独立して配色可能である。

これらの検討結果を表 5 に示す。この結果から、カラー菱形サブセル QR シンボルはカラーセル QR シンボルと比較して、データ容量（密度）が高いと言える。

表 5　データ容量の比較

項目	カラーセル QRシンボル	カラー菱形サブセル QRシンボル
サブセル形状		
互換部（中央部）	1ビット	1ビット
周辺部（格子部）8色時	2ビット	3ビット
合計	3ビット	4ビット

8. 電子署名の実装

上記で提案したカラー菱形サブセル QR シンボルに、電子署名データを収容できるかを検討する。

電子署名データは 160 ビットのデータが 2 組である。それを収容するには、8 ビットのデータコード語が 40 語必要となる。それらに対する誤り訂正率は、通常の QR コードで用いられている 15%から 25%を確保することが望ましい。

各ハッシュ値長に対する誤り訂正率 15%及び 25%とするに必要な訂正データコード語数を表 6 に示す。

表 6　訂正率毎の必要データコード語数

ハッシュ値長（ビット）	データコード語数	訂正データコード語数		合計コード語数	
		訂正率 15%	訂正率 25%	訂正率 15%	訂正率 25%
160	40	18	40	58	80
192	48	20	48	68	96
224	56	24	56	80	112
256	64	28	64	92	128

QR シンボルについて、各バージョンにおける各領域のデータコード語数を表 7 に示す。

① 白黒菱形サブセル QR シンボル

表 7 から、白黒の場合は、バージョン 3 では、63 データコード語を収容可能であるので、誤り訂正 15%の誤り訂正データコード語を含めて 160 ビットの電子署名データを収容可能である。

バージョン 4 では、224 ビット対応も可能である。一方、バージョン 2 以下では電子署名データを実装することができない。

② カラー4 色菱形サブセル QR シンボル

カラー4 色の場合は、バージョン 2 では 78 データコード語が収容可能であるので、誤り訂正 15%の誤り訂正データコード語を含めて 192 ビットの電子署名データを収容可能である。

③ カラー8 色菱形サブセル QR シンボル

カラー8 色の場合は、バージョン 1 では 72 データコード語が収容可能であるので、誤り訂正 15%の誤り訂正データコード語を含めて 192 ビットの電子署名データを収容可能である。

以上のように、白黒での符号化では、バージョン 1 及び 2 の場合、電子署名データを実装できなかったが、カラー化を行うことにより、実装することが可能となる。

表 7　菱形サブセルシンボルのデータコード語

バージョン（サイズ）	公開データ（中心部）コード語数	電子署名（格子部）コード語数		
		白黒	カラー4色	カラー8色
1 (21x21)	26	24	48	72
2 (25x25)	44	39	78	117
3 (29x29)	70	63	126	189
4 (33x33)	100	87	174	261

9. 処理アルゴリズム

菱形サブセルシンボルの符号化、復号は図 13 のシステム構成を前提にしている。

印刷システムは、認証局から秘密鍵と公開鍵を生成するソフトウェアをダウンロードし、それらを生成する。生成した秘密鍵は、システム内部に秘匿する。公開鍵と発行主体を認証局に送信して、公開鍵 ID を得る。公開鍵 ID は公開鍵と 1 対 1 に対応する ID である。

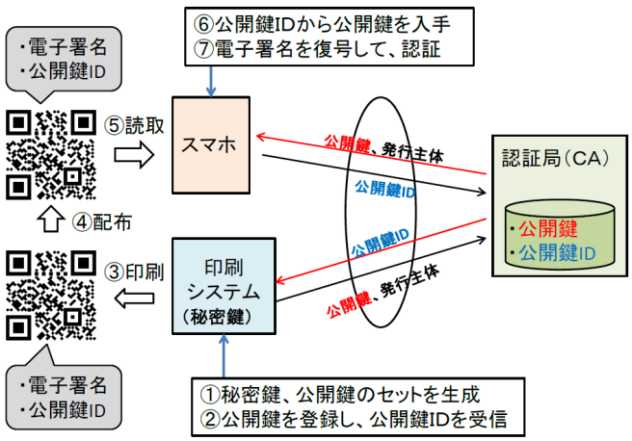


図 13　システム構成

9.1 データ構成

カラー菱形サブセル QR シンボルのデータの構成を表 8 に示す。ここで、d0 は通常のデータ部（互換部）に収容する公開データである。 d1 は d0 に対する電子署名データであり、d0 に対してハッシュ関数処理及び秘密鍵を用いた暗号化によって生成される。書式化データ fd0 は平文データ d0 を定められた書式に従って、データ種別毎にデータ圧縮などをした書式化データである。fd1 は電子署名データの書式化データである。

u0 は、fd0 を基に RS 符号で作成したデータコード語であり、データ部データコード語 u0、0 と訂正部データコード語 u0,1 から成る。同様に、u1 は fd1 を基に生成したデータコード語であり、データ部 u1,0 と訂正部 u1,1 から成る。

pu0 は u0 に対してパターンマスク処理を行った後のデータコード語である。

表 8　データ構成

	公開データ部（中央部サブセル）		電子署名部（格子部サブセル）	
	データ部	訂正部	データ部	訂正部
ユーザデータ	d0			
電子署名データ			d1	
書式化データ	fd0		fd1	
収容データコード語	u0		u1	
	u0,0	u0,1	u1,0	u1,1
マスク処理後収容データコード語	pu0			
	pu0,0	pu0,1		

9.2 符号化処理

ここでは、カラー菱形サブセル QR シンボルの符号化を行う場合の処理について説明する。

ここで、各領域に収容するデータを各サブセルと 1 対 1 に対応するデータコード語の作成をデータ符号化と呼び、それらのデータコード語を二次元シンボルとして光学特性に符号化する処理をシンボル符号化と呼ぶ。

ステップ 1　データの準備

公開データ部、電子署名部にそれぞれ収容する公開データ d0、電子署名 d1 を準備する。

公開データ d0 に対して、ハッシュ関数処理を行い、ハッシュ値データを得る。それを秘密鍵で暗号化して、160 ビット長のデータ Cd2,0 と Cd2,1 を得る。d1 はこの二つのデータであり、電子署名(ECDSA)である。埋め草部に公開鍵 ID と発行主体をセットする。

ステップ 2　公開データ部の符号化

公開データ部の符号化では、中央部サブセルを黒と白で符号化する。

①書式化

d0 をデータ圧縮などを行い書式化し、書式化データ fd0 を得る。

②RS 符号化

fd0 から公開データ部に収容するデータコード語 u0 を作成する。データ部データコード語 u0,0 に対して、RS 符号に基づいて誤り訂正部データコード語 u0,1 を作成する。

③パターンマスク処理

公開データ部のパターンマスクは、予め準備された 7 種類のパターンマスクについて演算を行い、定められたルールに従って、パターンマスクを選択し、選択されたパターンマスクによるパターンマスク処理を行い、pu0 を得る。

④公開データ部のシンボル生成

pu0 を収容する中央部サブセル部分のシンボル符号化を黒と白により行う。

このステップ 2 の処理は、通常の QR コードのシンボルを生成する処理と同じである。

ステップ 3　電子署名部の符号化

電子署名部の符号化では、格子部サブセルを黒青赤と白でシンボル符号化する。

①　電子署名の作成

公開データ d0 に対する電子署名 d1 を作成する。

d0 のハッシュ関数出力を、シンボル作成者の秘密鍵で暗号化し、電子署名データ d1 を得る。

②　書式化、RS 符号化

ステップ 2 の公開データ部の符号化と同様に、d1 から fd1 を作成し、u1 を作成する。

③　　電子署名部のシンボル生成

電子署名部ではパターンマスク処理を行なわない。ファインダーパターン（FP）と同一のパターンの出現は識別に影響を及ぼさないからである。また、特定色が格子部サブセル領域に部分的に集中し、または 4 色のサブセルの数がバランスしていなくても、中央部サブセルにパターンマスク処理がなされており、識別に影響を受けない。

u1 を収容する格子部サブセルから成るシンボル部分を生成する。u1 のサブセルのシンボル符号化は、左上部の格子サブセルから順に右側へ、そして次に下側のサブセルを符号化する。

u1 を 2 ビットずつに分割し、表 3 の色符号化テーブルに基づき対応する色を決定する。

以上で、カラー菱形サブセル QR シンボルの符号化処理が完了する。

9.3 復号処理

ステップ 1　画像撮影

シンボルを撮像する。得られた画像データから FP を用いてシンボルの存在を検出し、カラー菱形シンボル部の画像を抽出する。

ステップ 2　公開データ部の復号処理

①中央部サブセル色の判定

抽出した画像を通常の QR コードとして識別し pu0 を得る。次に、パターンマスク解除処理を行い u0 を得る。

②RS 符号の復号

u0 を基に、RS 符号の誤り訂正処理を行い、fd0 を経て、d0 を得る。ステップ 2 の処理は、通常の QR コードの復号処理と同じである。

ステップ 3　電子署名部の復号

①　格子部サブセル色の判定

中央部サブセルと同様に、格子部サブセルを識別し、u1 を得る。

ここで、格子部サブセルは 4 色を用いて符号化されており、その符号化色の特定が必要となる。ここでは、格子部

サブセルを検出して得た RGB 値から R 成分と B 成分の有無を判別して、表 3 の符号化テーブルから 2 ビットを得る。この処理を格子部サブセルを符号化した順に行うことにより、u1 を得る。

②RS 符号の復号

u1 を基に、RS 符号の誤り訂正処理を行い、fd1 を経て、d1 を得る。

以上の処理により、公開データ d0 及び電子署名データ d1 を得る。

ステップ 4　認証

①　公開鍵の取得

ステップ 2 で復号した公開データ部の書式化データ fd0 の埋め草領域から公開鍵 ID を読出し、ネットワークを経由して認証局に当該公開鍵 ID を送信して、公開鍵と発行主体を得る。

②　認証処理

取得した公開鍵を用いて、電子署名データ d1 からハッシュ値 h0 を得る。公開データ d0 から符号化処理のステップ 1 で行った処理（ハッシュ関数処理）を行い H0 を得る。h0 と H0 及び発行主体が一致していれば、認証できたとする。

10. 紙媒体に電子署名を付す意義

従来、電子署名はディジタルデータに付され、その存在場所はコンピュータや記憶装置の内部に限定されていた。それに対して、電子署名付き QR シンボルを用いることにより、紙に電子署名を付すことが可能になった。

紙媒体に印刷されている情報と同じ情報が QR シンボルに記憶され、その情報に対して電子署名が生成され、付されており、その作成者名が表示されていれば、その紙媒体の内容と作成者を認証可能である。

例えば、紙幣に適用する場合には、額面と記番号を QR シンボルの公開データ部に記憶し、それらに対して予め登録された発行主体（中央銀行等）の秘密鍵で電子署名データを作成して、電子署名部に記憶させれば、その紙幣の認証、真贋判定を行うことができる。

11. 応用システム

QR シンボルに電子署名を有することにより、ユーザデータ部の改ざん、偽造を検出可能であり、作成者の認証が可能となった。これらの機能を活かすシステムについて検討する。

電子署名付き QR シンボルの活用方法として、紙に印刷して用いる場合とスマホなどの画面に表示して用いる場合がある。これらのそれぞれの利用形態について述べる。

11.1 紙印刷での応用

前節で紙媒体に電子署名を付す意義について延べ、紙幣の認証を例に挙げた。同様な応用を想定することが可能であり、それらを表 9 に示す。

第 1 の応用は、紙幣と同様に、書面自体を認証する場合であり、証明書や契約書などに電子署名付き QR シンボルを付して、当該書面を認証する。

第 2 の応用は、シールや包装に電子署名付き QR シンボルを付して、商品に貼付し、包装する場合である。この場合には、包装等を介して商品の認証が可能であり、医薬品などの真贋判定に用いる。

第 3 の応用は、書面内容の認証である。現在、QR コードに WEB アドレスを記憶させ、それをスマホで読取らせて WEB 参照を行うことがなされている。しかし、フィッシングなどの脅威が存在している。そこで、WEB アドレスに電子署名を付せば、WEB アドレス及びその作成者の認証が行えるので、それらの脅威を回避可能である。

表 9　紙印刷での応用

応用の範囲	具体的内容
書面自体の認証	証明書（社員証、資格証）、契約書（電子印鑑）、有価証券（紙幣）
貼付対象の認証	偽造防止（医薬品、一般商品）
書面内容の認証	WEB参照（フィッシング防止）、キャッシュレス決済（MPM）

11.2 画面表示での応用

紙印刷での応用では、印刷された後、比較的長時間利用が継続され、繰り返し読取りが行われる。それに対して、画面表示での応用は、最新の情報を表示し、その表示は読取りがなされた後には直ちに消去され、その利用は 1 回のみであることが特徴である。また、赤や青の再現性が高く、経時劣化がないので、カラーシンボルの表出に適している。画面表示での応用を表 10 に示す。

第 1 の応用は、表示内容を認証である。表示した内容と作成者を認証を行う。CPM 方式のキャッシュレス決済や各種の会員証の表示に用いる。

第 2 の応用は、限定権限付与である。この典型的な利用は入門証である。特定の期間を限定して、入門を許可するので、当該許可された期間以外では入門することができない。ホテルの部屋の鍵としての利用も同じ利用形態である。

表 10　画面表示での応用

応用の範囲	具体的内容
表示内容の認証	キャッシュレス決済（CPM）、会員証
限定権限付与	入門証

12. おわりに

通常の QR コードと互換性を有し、アプリケーションソフトに全く影響を与えずに電子署名を実装するカラー菱形サブセルを用いたシンボルを提案した。QR コードと互換性のある既存のカラーセル QR シンボルと比較し、ロバストネスが向上し、データ密度が高いことを示した。また、カラー化によって、小さなバージョンのシンボルにおいても、ECDSA の電子署名を付すことを可能とした。小型のシンボルにおいて電子署名による安全な受渡しが可能となることにより、広範囲のより高いセキュリティ性が要求される用途に QR シンボルが適用可能となる。

格子部のデータ収容能力は、カラー化により増大し、バージョンの大きなシンボルでは、電子署名データを収容しても未使用のデータ領域が残る。そこで、今後、格子部のデータ構造を設定し、秘匿データを収容する等の活用を検討していく。

参考文献

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

[2] Katharina Krombholz、 Peter Frühwirt、 Peter Kieseberg、 Ioannis kapsalis、 Markus Huber、 Edgar Weippl、 QR Code Security: A Survey of Attacks and Challenges for Usable Security、 International Conference on Human Aspects of Information Security、 Privacy、 and Trust; HAS 2014: pp 79-90、 2014。

[3] Ms。 Pranoti Panchal、 Prof。 Savitri Patil。 Android Mobile Security using Secure Hash Algorithm、 IJCSMC、 Vol。 5、 Issue。 1、 January 2016、 pg。226－232、 2016。

[4] Riccardo Focardi 、 Flaminia L。 Luccio 、 Heider A。 M。 Wahsheh 、 Usable Cryptographic QR Codes、 2018 IEEE International Conference on Industrial Technology (ICIT)、 2018。

[5] Maykin Warasart 、 Pramote Kuacharoen 、 Paper-based Document Authentication using Digital Signature and QR Code 、 4TH International Conference on Computer Engineering and Technology (ICCET 2012)、 2012。

[6] Faisal Razzak 、 Spamming the Internet of Things: A Possibility and its probable Solution 、 Procedia Computer Science Volume 10、 2012、 Pages 658-665、 2012。

[7] Vaidhyesh P 。 S 、 SECURING IoT DEVICES BY GENERATING QR CODES、 International Journal of Pure and Applied Mathematics Volume 119 No。 12 2018、pp 13743-13749、 2018。

[8] A Wibiyanto 。 I Afrianto、 QR code and transport layer security for licensing documents verification、 IOP Conf。 Series: Materials Science and Engineering 407 (2018) 012069、 2018。

[9] 柏井祐樹、 渡辺優平、森井昌克、 オフラインサイト認証可能な QR コード、FIT2012(第四分冊 107)、 2012。

[10] 先名健一、個人認証機能を有するデジタル署名型 QR コード、信学技報、 117(39)、 EMM2017－11（2017－05）p。61-66、 2017。

[11] 寺浦 信之、 越前 功、岩村 惠市、 菱形サブセルを用いた QR シンボルの互換性を保つ領域分割による容量拡大と電子署名の実装検討、 コンピュータセキュリティシンポジウム(CSS2019)、 p。17-24、 2019。

[12] H。 Kato、 K。 Tan、 D。 Chai、 Development Of A Novel Finder Pattern For Effective Color 2D Barcode Detection、 Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications。 ISPA '08。 (pp。 1006-1013)。 Sydney、 Australia。 IEEE Computer Society、2008

[13] 助川 修司、QR コードの多色化による 2 次元コードの大容量化について、情報処理学会全国大会講演論文集第 70 回平成 20 年(4)、 845-846、 2008

[14] 寺田 遼平、藤本 敬介、中山 泰一、カラー二次元コードを高解像化するための認識アルゴリズムの実現と評価、信学技報、SS2008-57、2009-3

[15] 遠藤祐介、廣友雅徳、佐治勇樹、渡辺優平、森井昌克、多値二次元コードにおける高階調度認識アルゴリズムの提案、電子情報通信学会論文誌 D Vol。J95-D No。11 PP。1935-1943

[16] 寺浦 信之、櫻井　幸一、秘匿領域を有する多値セル構造の二次元コードの互換性と識別性のスマートフォン実装による評価、コンピュータセキュリティシンポジウム(CSS2014)、 1276-1283、 2014。

[17] 寺浦 信之、櫻井 幸一、秘匿領域を有する高密度二次元コードの互換性と識別性に関するスマートフォン実装による評価、2015 年暗号と情報セキュリティシンポジウム(SCIS2015)、 1B2-2、 2015

[18] 寺浦 信之、櫻井 幸一、‘セルの微細分割による二次元コードの情報ハイディング’、第 11 回情報科学技術フォーラム(FIT2012)、 571-578、 2012