

# 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

寺浦 信之<sup>†1</sup> 越前 功<sup>†2</sup> 岩村 恵市<sup>†3</sup>

**概要:** QR シンボルに記憶させたデータをスマートフォンで読み取り、WEB の参照や、読取った口座に支払い金額を振り込むことがなされている。しかし、現在の QR シンボルは、誰でも簡単に作成することが可能であり、なりすましや偽造が容易に実行可能である。その対策の一つとして、QR シンボルに電子署名を実装することがある。互換性の観点から、電子署名はアプリデータとは独立した記憶領域に実装する分離性が必要である。従来、独立した記憶領域を付加する手法には、セルそのものの多値化手法が提案されてきた。それに対して、互換性に影響を与えないセルの周辺領域へのサブセルの埋め込み手法を開発した。すなわち、既存の正方形セルを菱形サブセルに領域分割し、分離した記憶領域を生成した。提案するシンボルの構造とその領域に ECDSA の電子署名を実装する手法について報告する。

**キーワード:** QR シンボル, 菱形サブセル, 領域分割, 互換性, 分離性, ECDSA

## Capacity Expansion by Area Division Maintaining Compatibility of QR Symbol using Rhombic Subcell and Implementation of a Digital Signature

Nobuyuki Teraura<sup>†1</sup> Isao Echizen<sup>†2</sup> Keiichi Iwamura<sup>†3</sup>

**Abstract:** After reading the data stored in the QR symbol with a smartphone, the WEB is referenced and the payment amount is transferred to the read account. However, anyone can easily create the current QR symbol, and impersonation and forgery can be performed easily. One countermeasure is to implement a digital signature on the QR symbol. From the viewpoint of compatibility, digital signatures must be separable to be implemented independently of application data. Conventionally, as a method of adding an independent storage area, a multivalued method of the cell itself has been proposed. On the other hand, we developed a method for embedding subcells in the peripheral area of cells that does not affect compatibility. That is, the square cell was divided into rhombus subcells to generate separate storage areas. In this paper, we report on the proposed symbol structure and the method to implement ECDSA digital signature in the domain.

**Keywords:** QR symbol, Rhombus subcell, Area division, Compatibility, Separability, ECDSA

### 1. はじめに

#### 1.1 セキュリティ性の実現

現在の QR シンボル[1]は、誰でも簡単に作成することが可能であり、なりすましや偽造が容易に実行可能である。その対策の一つとして、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。その多くは、アプリデータと電子署名を同じ領域に記憶するものであった。しかし、互換

性の観点から電子署名はアプリデータとは分離した記憶領域に実装されることが望ましい。そこで、互換性に影響を与えることなく正方形セルを菱形サブセルに領域分割し、分離した記憶領域に ECDSA を実装する手法を検討した。

#### 1.2 既存の研究

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] [3] [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] [6] [7] [8]。これらは、通常の QR シンボルをそのまま使い、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

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

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.

また, 著者等は, 黒セルを4分割したサブセルを二重符号化するシンボルに埋め込む提案をしている[11] .

### 1.3 既存研究の課題

[9]での RSA 電子署名は 2048 ビットのデータ量を有し, それらを埋め草領域に記憶するので, シンボルサイズが大きくなり, 実用されているサイズとかけ離れている. [10]では, 誤り訂正を用いてデータを抽出しており, 実際に発生する誤りが電子署名データに混入する可能性がある.

[11]では, セルを4分割したサブセルを符号化の基本単位としているため, サブセル面積がセル面積の4分の1となり. 同一サイズのシンボルと比較すると, 識別性に劣ると言える.

### 1.4 本提案の電子署名の効果

#### ①QR シンボルの脅威

情報セキュリティにおける4大脅威は, 盗聴, なりすまし, 改ざん, 否認である. これらの脅威と QR シンボルへの脅威との対応を表1に示す.

盗聴は秘匿データの読出しに対応し, なりすましは偽造, 複製, 複写に対応する. QR シンボルでは RS 符号を用いた誤り訂正機能があるので, 一度印刷されたシンボルを改ざんすることはできない. すなわち, 黒セルや白セルを何らかの手段で反転させたとしても, 誤り訂正の範囲内であれば, 反転させた部分は訂正され, 正規のデータが読み出せる. また, 誤り訂正の範囲外であれば誤りが検出され, 正規のデータ以外が復号される可能性はない.

#### ②電子署名の効果

QR シンボルに対する脅威は, 表1に示すように, その用途によって異なる. しかし, 電子署名の効果は共通であり, 偽造, 改ざんと否認の防止である.

表1 本提案の電子署名の効果

脅威		WEB参照	偽造防止	QR決済
盗聴	秘匿データ読出	—	×	×
なりすまし	偽造	○	○	○
	複製	—	×	—
	複写	—	△	—
改ざん	データ部変更	○	○	○
否認		○	○	○

○: 効果有り ×: 効果無し △: 付随効果 —: 脅威無し

## 1.5 貢献

本提案は, QR シンボルに ECDSA を実装することにより, QR シンボルにセキュリティを付与し, QR シンボルに関するセキュリティ問題の低減を可能とする. 偽造や否認を防止し, 発行者認証, 安全な WEB 参照, QR 決済を実現する.

## 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 シンボルの通常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, 電子署名付き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.

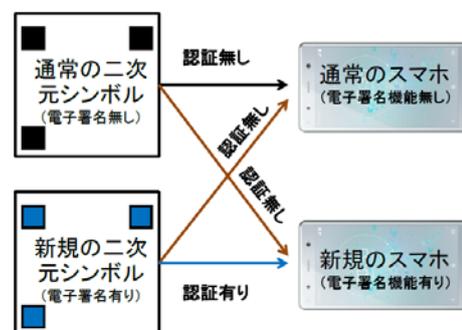


図1 互換性

### 2.2 読取り性

QR シンボルには, 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. バル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. 電子署名付き 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いるからである. 電子署名データも, データ領域に収容されていればアプリソフトが意識する必要があるため, 通常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.

## 3. ECDSA の採用

QR シンボルでは, 実用的なサイズに制限があり, 大きなデータ量の電子署名を収容することができない. ECDSA は RSA 電子署名に比べて十分の1のデータ量で同等の安全性を有するとされており ECDSA を採用する.

## 4. 電子署名の実装シンボルの検討

### 4.1 記憶領域の拡大

同じバージョン（シンボルの構成）のシンボルの記憶容量を、互換性を維持して拡大する手法には、符号化の基本単位であるセルそのものの多値化手法と本論文で提案するセル間へサブセルを挿入する領域分割手法がある。

### 4.2 セルの多値化

セルの多値化には、多色化と多領域化がある。

#### (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、4色（2ビット）や8色（3ビット）を用いて符号化を行う[12]。また、暗色セルのみを暗色系の二色を用いて再符号化する二重符号化手法も提案されている[13]。

#### (2)多領域化

一方、多領域化は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[14]。また、多色化と多領域化は同時に用いる提案もなされている[11][12]。

セルの多値化を用いて記憶容量を拡大した例を表2に示す。

表2 セル多値化のQRシンボル

符号化対象	暗色セルと明色セル			暗色セル
	単色	8色	4色	3色
単領域				
多領域				

### 4.3 領域分割

本論文で提案する領域分割法について述べる。

#### (1)セル周辺部の影響

QRシンボルは、図2に示すように正方形のセルを符号化の基本単位とするマトリックス型の二次元シンボルである。セルには収容するデータとは関係せず、常に固定された同一の黒または白である固定セルと収容するデータに応じて黒または白となる変動セルがある。変動セルが黒または白のいずれかを識別するために、セル画像のサンプリングが行われる。サンプリングされるのはセルの中心点である。撮像されたシンボル画像は、手振れ、ピンボケにより周辺セル色がセルの周辺部を侵食している。また、サンプリング画像がJPEG画像として圧縮された形式でスマホ識別ソフトに提供されるため、平均化処理がなされており、周辺

セル色がセルの周辺部を侵食する。従って、セルの中心部が他の点と比較して、周辺部のセル色の影響が一番少ないと言える。

また、サンプリングを行う点は、QRシンボルの画像のゆがみ等の影響で、セルの中心点のまわりに分布し、中心点から離れるにしたがって、サンプリング位置となる確率は低くなる。そこで、図3に示すセルの外周に接する円の内部が主に黒または白の符号化を担っており、セル内の円の外側は符号化及びサンプリング点への寄与は小さい。また、図4に示すように円の半径を小さくしても、セルサイズが一定程度大きい場合には、その識別力は低下しないと考えられる。

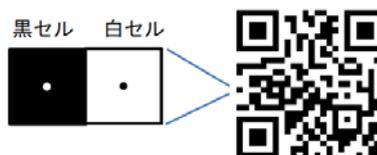


図2 QRシンボルの正方形セル



図3 円形セル

図4 円形サブセル

#### (2)予備実験

上記で述べた識別力を評価するために、読取試験を行った。読取試験を行ったシンボルを図5、図6、図7に示す。図5は通常のQRシンボルであり正方形のセルを符号化している。図6、図7は円形サブセルを符号化しており、円の半径をセル一辺の約0.7倍に小さくしている。また、図6に示すシンボルでは円の外側のセル領域（背景）は白であるが、図7に示すシンボルではその領域を黒としている。これらについての読取結果を図8に示す。読取り試験の条件については、第7章で述べる。



図5 通常のQRシンボル



図6 QRシンボル(背景白) 図7 QRシンボル(背景黒)

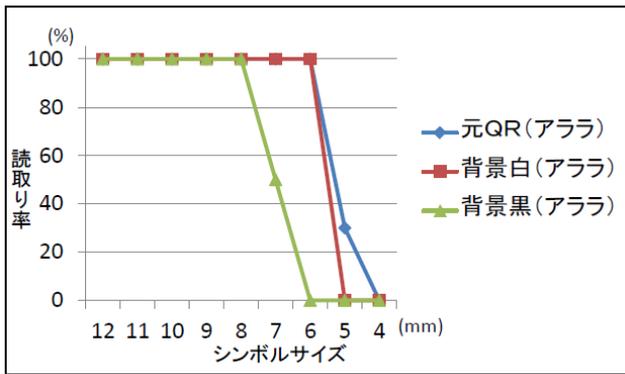


図8 予備実験の読取り率

この読取試験の結果、元の QR シンボルと背景が白の円形セルを比較すると、両者ともにセルサイズが 0.24 ミリ（シンボルサイズ 6 ミリ）まで、100%読取り可能であり、ほぼ同じ読取り率であった。この結果は、黒サブセルの面積が 38%となっても、読取り限界がほぼ同じであることを示している。また、背景が黒の円形セルの場合には、セルの大きさが 0.32 ミリ（シンボルサイズ 8 ミリ）まで 100%読取り可能であった。

この結果は、円の外側が全面白色または全面黒色でも円の中心部のサンプリングには、一定程度の大きさのセルの場合には、影響を及ぼさないことを示している。また、背景が黒の円形セルの印刷状況を観察したところ、背景の黒が白サブセルに侵食しており、小さなシンボルの場合、実質的な白サブセルの面積が低減されているのが観測された。

#### (4)サブセル挿入の影響

上記の結果から、セルの中心を中心点とする円の外側にはどのような配色がなされていても、その円に配色された色の識別に影響がないので、そこに同じく円を設定し、それを白または黒に配色しても、影響がないと言える。

#### (5)サブセルの検討

セルの中央を中心とする符号化単位を中央部サブセルと呼ぶ。また、中央部サブセルの間に挿入される符号化単位を周辺部サブセルと呼ぶ。中央部サブセルと周辺部サブセルは、識別力が同じであることが必要である。そのためには、中央部サブセルと周辺部サブセルの形状と大きさは同じであることが必要条件となる。

この条件を満たす領域分割には二つの形式が存在する。二分の 1 モデルと四分の 1 モデルである。サブセル形状を円とした場合の構成をそれぞれ図 9、図 10 に示す。

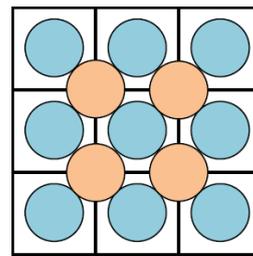


図9 二分の 1 モデル

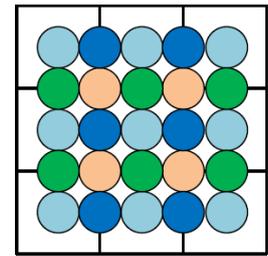


図10 四分の 1 モデル

二分の 1 モデルは、正方形のセルの角部、すなわち外周が交差する格子点を中心点とするサブセルを挿入、配置するものである。それに対して、四分の 1 モデルは、格子点に加えて、セル外周部の横線中央部と縦線中央部に合計三つのサブセルを挿入、配置した形状である。

#### (6)サブセル形状の検討

図 9 に示す二分の 1 モデルのサブセル構成では、中心部サブセルと格子部サブセルの円の外側に符号化に用いられていない領域が存在する。それらの領域を図 11 のように、隣接するサブセルに収容すると、図 12 に示す菱形形状となる。

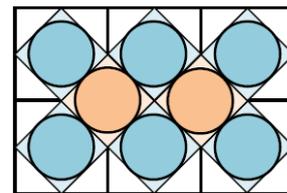


図11 未利用部分の収容

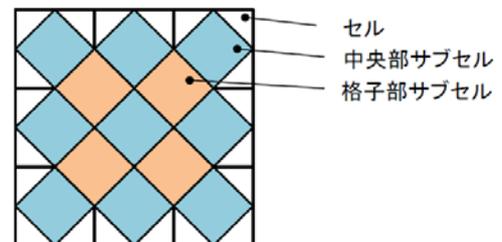


図12 二分の 1 モデルサブセル構成

また、図 10 に示す四分の 1 モデルでも同様に未使用領域を隣接するサブセルに収容すると図 13 に示す正方形のサブセルとなる。

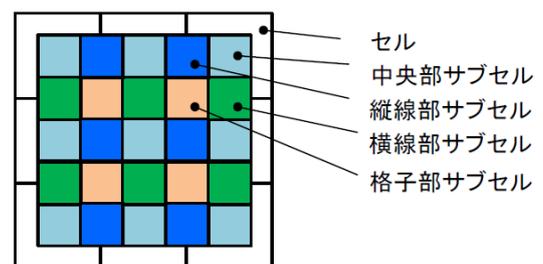


図13 四分の 1 モデルサブセル構成

ここで、図 13 の右上の 4 つのサブセルをセルの内部に収容する構成も想定可能である。しかし、この場合は、セルの領域分割となり、互換性が失われる。セルの中央部に対応する符号化部が存在しないからである。

(7) 菱形サブセルの採用

二分の 1 モデルの菱形サブセルと四分の 1 モデルの正方形サブセルを比較すると四分の 1 モデルの正方形の面積は二分の 1 モデルの菱形サブセルの面積の半分であり、比較的小さなセルの場合には、識別力は劣ると想定される。また、シンボルサイズが比較的大きな場合には、新しい記憶領域を生成することが可能であり、秘匿データを収容する場合には有用である。

本論文の目的は ECDSA を収容することであるので、ここでは二分の 1 モデルの菱形サブセルについて、議論を進めることとする。

(8) シンボルの構成

前記のように、QR シンボルでは固定セルと変動セルがある。固定セルはシンボルの存在検出や歪み補正などに用いられ、既存ソフトは正方形のセルを前提としてしているのでセル形状を保持し、変動セルのみ領域分割を行う。

このような方針で QR シンボルを構成した例を図 14、図 15 に示す。図 14 は中心部サブセル、格子部サブセルの暗色部を黒で表現したものであり、図 15 は格子部の暗色部を赤で表現したものである。

菱形サブセルを用いて 2 領域分割を行ったシンボルを以下では菱形シンボルと呼ぶ。



図 14 領域分割 QR シンボル 図 15 格子部を赤で表現

5. 電子署名の実装検討

上記で提案した菱形シンボルに、ECDSA データを収容できるかを検討する。

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 3 に示す。ECDSA のデータは 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データコード数も同数程度とする。同数の場合には、誤り訂正率 25% となる。

表 3 から、バージョン 1 以外では、初期の誤り訂正率で ECDSA データを収容可能である。また、バージョン 4 以上

では、訂正コード語に加えて余り語数が発生するので、秘密データを収容することも可能である。

バージョン 2 では、格子部のコード語は 39 語であり、ECDSA データを収容できないが、二重符号化を行うことより収容可能となる。バージョン 3 では、格子部のコード語数は 65 語であり、訂正用コード語を 25 語確保（訂正率 20.8%）して ECDSA データを収容可能である。

表 3 菱形シンボルの ECDSA 実装時のデータコード語

バージョン (サイズ)	互換部 (中心部) コード語数	追加部 (格子部) コード語数	二重 符号化部 コード語数	誤り訂正 (二重符号化部を含む)	
				訂正コード 語数	誤り訂正率 (%)
1 (21x21)	26	24	25	-	-
2 (25x25)	44	39	41	(40)	(25)
3 (29x29)	70	65	62	25(80)	20.8(33.3)
4 (33x33)	100	87	93	47(80)	25.9(33.3)

6. 処理アルゴリズム

ECDSA データ付き菱形シンボルの符号化、復号は図 16 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。

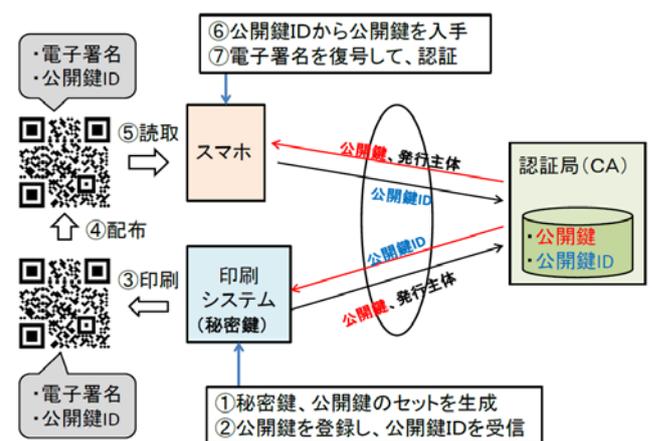


図 16 システム構成

6.1 データ構成

ECDSA データ付き菱形シンボルのデータの構成を表 4 に示す。ここで、d0 は通常データ部（互換部）に収容するユーザーデータであり、d1 は ECDSA データである。書式化データ fd0, fd1 はユーザーデータ d0 及び ECDSA データ d1 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。

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, 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[1]を行った後のデータコード語である。

表 4 データ構成

	互換部 (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		d1 (cd1,0 cd1,1)	
書式化データ	fd0		fd1	
收容データ コード語	u0		u1	
	u0,0	u0,1	u1,0	u1,1
マスク処理後 收容データ コード語	pu0		/	
	pu0,0	pu0,1		

## 6.2 符号化処理

ここでは, ECDSA データ付菱形シンボルの符号化を行う場合の処理について説明する。

### ステップ 1 データの準備

互換部, 電子署名部に收容するユーザデータ d0 及び ECDSA データ d1 を準備する。

d0 に対して, ハッシュ関数処理を行い, 160 ビット長のデータを得る。秘密鍵で暗号化して, 160 ビット長のデータ Cd1,0 と Cd1,1 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 互換部の符号化

互換部のセルの符号化では, 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 から互換部にセット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

互換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互換部のシンボル生成

pu0 を收容する中央部サブセルから成るシンボルの一部を生成する。このステップ 2 の処理は, 通常の QR シンボル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, 電子署名部を構成する格子部サブセルを黒と白で符号化する。

#### ①書式化, RS 符号化

ステップ 2 の互換部の符号化と同様に, d1 から fd1 を作成し, u1 を作成する。

#### ②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わない。ファイナダーパターン (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, 黒または白のパターンが格子部サブセル領域に部分的に集中しまたは黒と白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 を收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。

このステップ 3 の処理は, 通常の QR シンボルのシンボルを生成する処理と, 格子部サブセルの配置及びパターンマスク処理を除いて同じである。

以上で, ECDSA 付き菱形シンボルの生成が完了する。

## 6.3 復号処理

### ステップ 1 画像撮影

菱形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, 菱形シンボル部の画像を抽出する。

### ステップ 2 互換部の復号処理

#### ①中央部サブセル色の判定

抽出した画像を既存の QR シンボルとして識別し, pu0 を得る。そして, 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 シンボル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サブセル色の判定

上記の符号化の順に, 格子部サブセルを識別し, 黒を 1 白を 0 として u1 の 1 ビットを得る。この処理を全ての格子部サブセルについて行い, 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, ユーザデータ d0 及び ECDSA 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で復号した互換部の書式化データ fd0 の埋め草領域から公開鍵 ID を読み出し、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、ECDSA データ d1 からハッシュ値 h0 を得る。ユーザデータ d0 から符号化処理のステップ1で符号化処理をした同様の処理（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。

## 7. 読取試験

菱形シンボルの読取試験を実施した。読取試験の条件を表5に示し、読取試験結果を図17に示す。

表5 読取試験条件

項目		読取条件
印刷	プリンタ	キヤノン(TS8230)
	用紙	コクヨ(マット紙:0.15mm)
読取り	機器	SONY(エクスペリアSO-03G)
	ソフト	①QRコードリーダーQ(アララ提供) ②ICタグ・バーコードリーダー(NTTドコモ提供)
	試行回数	各10回

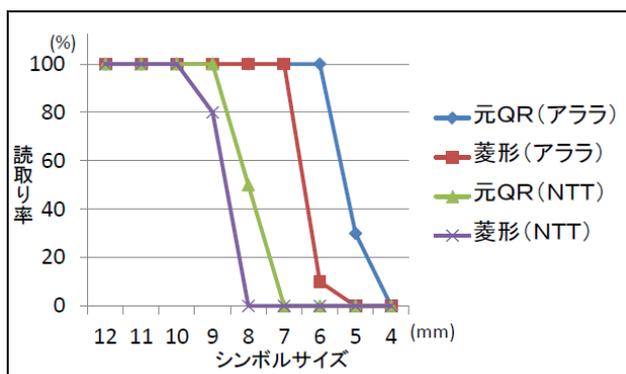


図17 読取試験結果

読取りには既存のQRシンボル用の読取りソフトを用いた。そこで、読取り対象は中央部サブセルである。格子部サブセルについては、専用の読取りソフトウェアが必要であり未実施である。格子部サブセルは、中央部サブセルと全く同じ条件（同一形状、同一サイズ）であり、同じ読取

り特性が得られると考えられる。

読取試験に用いた二つのソフトウェアで、読取結果に差が生じた。これは読み取れなかった場合のエラー処理等読取りアルゴリズムの差によるものと考えられる。両者共に元のQRシンボルと菱形シンボルとの識別結果に大差がなく、わずかに菱形シンボルの読取り限界値が大きい結果であった。読取試験に用いたバージョン2では、通常10~15mm程度のサイズが用いられている。読取試験の結果から、それらは十分読取り可能であり、実用性を確認できる。

## 8. 四分割二重符号化シンボルとの比較

著者等は、電子署名を内蔵するQRシンボルとして、4分割二重符号化シンボルを提案している[10]。このシンボルと本提案の菱形サブセルによる2領域分割シンボルとの比較を表6に示す。

表6 4分割二重符号化シンボルとの比較

		4分割二重符号化	本提案
共通事項		①互換性 ②分離性 ③電子署名(ECDSA)内蔵	
個別事項	記憶容量 (QRコード比率)	3倍	2倍(標準) 3倍(二重符号化)
	サブセル面積	セルの四分の1	セルの二分の1
	視覚互換性	有り*	無し
	白黒センサー読取	不可	可能(標準)

\*赤外線吸収黒インクと赤外線透過黒インクで符号化の場合

両シンボルは異なる特長を有するので、用いられるシステムによって、使い分けが可能である。本提案のシンボルでは、視覚互換性が失われる。一方、サブセル面積が大きく識別力が高いにも関わらずデータ密度が向上している。この理由は、4分割二重符号化では、サブセル面積が小さいためシンボルサイズが比較的大きくなり、黒セルのみを二重符号化する一方、菱形シンボルではセル周辺の不寄与領域に格子サブセルを埋め込み、不寄与領域を活用していることである。

## 9. 応用システム

### 9.1 WEB参照

WEB参照用途では、作成者を偽った悪意のWEBに誘導される可能性があるが、ECDSA付菱形シンボルを用いて作成者を認証することにより、フィッシングなどの可能性を回避することができる。

### 9.2 有価証券、医薬品、証明書の偽造防止

商品券やコンサートチケットなどの有価証券や高額な医薬品の偽造防止用途にも電子署名は有用である。有価証券

では、発行元を認証し（なりすまし防止）内容が偽造、改ざんされていないことが確認可能となる。医薬品では、製造元の認証や内容物の保証が可能となり、偽造防止を図ることができる。この用途では、コピー防止の重要性によって赤外線特性を用いた印刷も可能である。

電子署名を実装した二次元シンボルの最大の特徴は、発行者認証が可能である点である。この特徴を活かした応用として社員証など発行者が何らかの証明を行う用途があり、それらを第三者がスマホ等を用いて確認、認証を行う。

### 9.3 スマホ決済

店舗側から提示された QR シンボルをスマホで読取る MPM 型のスマホ決済への応用を図 18 に示す。支払いを受ける側の電子署名が入っていれば、なりすましを防げる。例えば、レンタル自転車に貼られている QR シンボルを読取り、レンタル料を支払うシステムでは、QR シンボルを何者かが異なる支払い先を指定する QR シンボルに張り替える事件が発生している。これらは発行元の電子署名による認証を行うことで防止可能である。



第 18 図 MPM 型決済システム

## 10. 互換性を維持した電子署名実装の意義

菱形シンボルは前記のように既存の QR シンボルと互換性の維持を前提に案出されたシンボルであり、確認試験によって互換性を示した。

この互換性によって、現在用いられている QR シンボルを本シンボルに逐次代替可能である。既存の読取り装置で本シンボルを読む場合には、電子署名部分を読取れないため、認証は行えないが従前の処理は可能である。一方、今後提供していくソフトウェアを用いることにより、電子署名を用いた認証が可能となる。本シンボルが用いられる場合、既存の QR シンボル及びシステムと共存が可能であり、逐次に使用を拡大することが可能となる。

## 11. おわりに

既存の QR シンボルと互換性を有し、アプリケーションソフトに全く影響を与えずに ECDSA を実装する菱形サブセルを用いた 2 領域分割手法を提案した。ECDSA を実装することにより、発行者の認証を可能とし、互換部のデータが偽造されていないことが検証されるなどのセキュリティ性を QR シンボルに付与することができた。

現在、符号化ソフト及び復号ソフトの開発を進めており、

実験結果が出た時点で報告を行う。

## 参考文献

- [1]ISO/IEC 18004:2006 Information technology -- Automatic identification and data capture techniques -- QR Code 2005 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 恵市, サブセル分割二重符号化を用いた QR シンボルへの電子署名の互換性を保つ実装検討, 信学技報, 118(494), EMM2018-113 (2019-03), p.117-122, 2019.
- [12]寺浦信之, 櫻井幸一, 多値セル型二次元コードでの多分割領域への複数ユーザのアクセス制御, 情報処理学会論文誌, “Vol.57, No.9, pp.1965-1973, 2015.
- [13]寺浦 信之, 岩村 恵市, 越前 功, 櫻井 幸一, 二重符号化二次元コードのパターンマスク秘匿化への RS 符号を用いた誤り訂正の影響検討, 信学技報, 117(40), EMM2017-11 (2017-05), p.67-72, 2017.
- [14]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.