2019年度　修士論文発表会

菱形サブセルを用いる電子署名を追加した安全なＱＲコードの研究

WANG　CAN

2722182006

明治大学大学院

先端数理科学研究科

先端メディアサイエンス専攻

菊池研究室

背景

・ＱＲコードは世界に広く普及している

入場券、アプリの登録、決済サービスなどに使われている

・2011年10月にＱＲコードを介して、料金を発生させるマルウェアが発見された[1]

・2018年[2],2019年[3]中国で、店のＱＲコードが貼り替えられ、ほかの口座に振り込まれた

[1] https://scan.netsecurity.ne.jp/article/2011/10/13/27439.html
[2] https://www.fnn.jp/posts/00401501HDK
[3] https://www.guancha.cn/politics/2019_12_04_527319.shtml

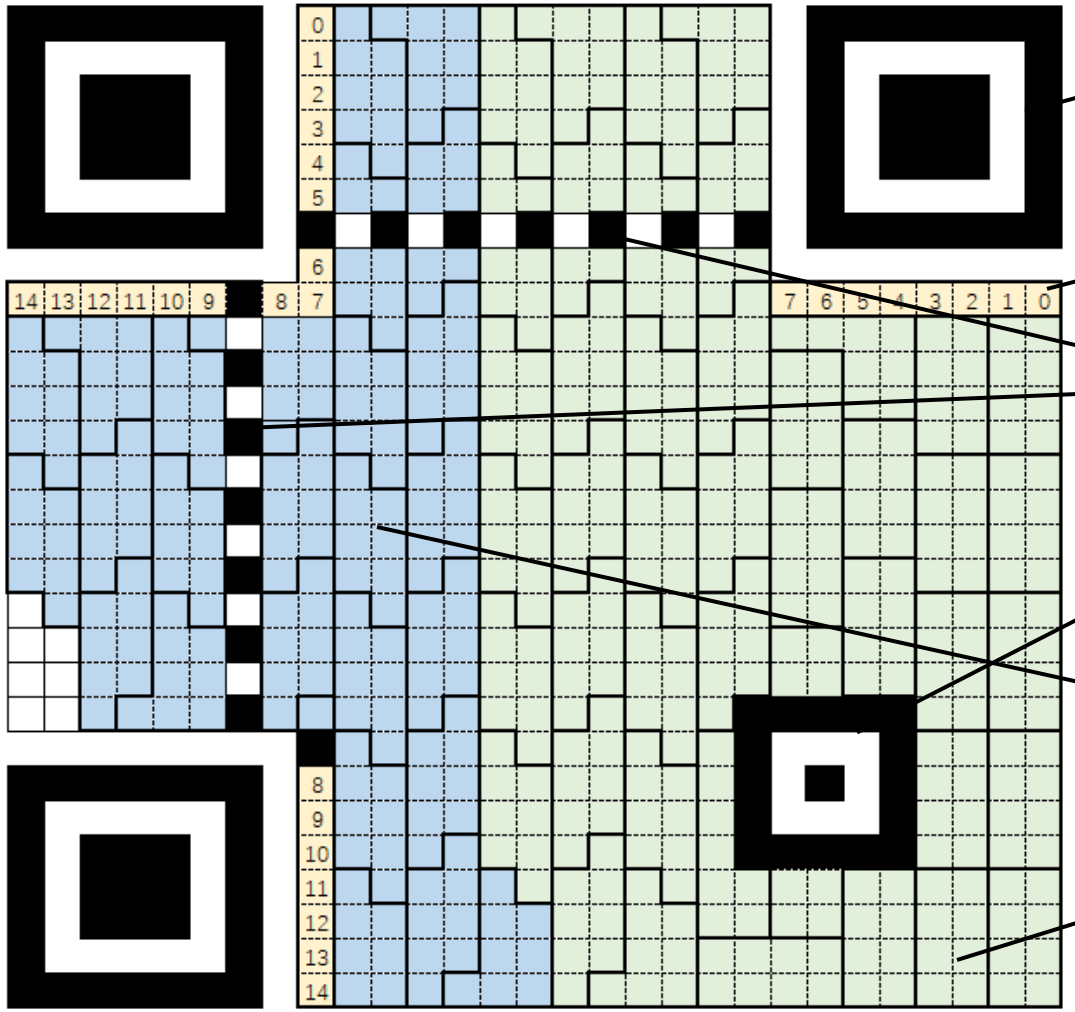
目的

ＱＲコードの安全性を高める

↓

QRコードに電子署名を追加する

ＱＲコードの仕様



位置検出パターン

形式情報

タイミングパターン

位置合わせパターン

機能パターン

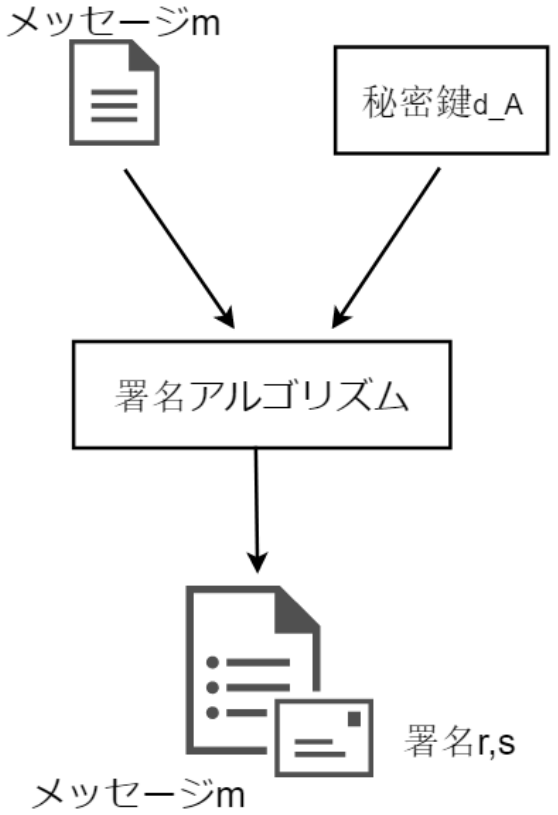
誤り訂正コード語

データコード語

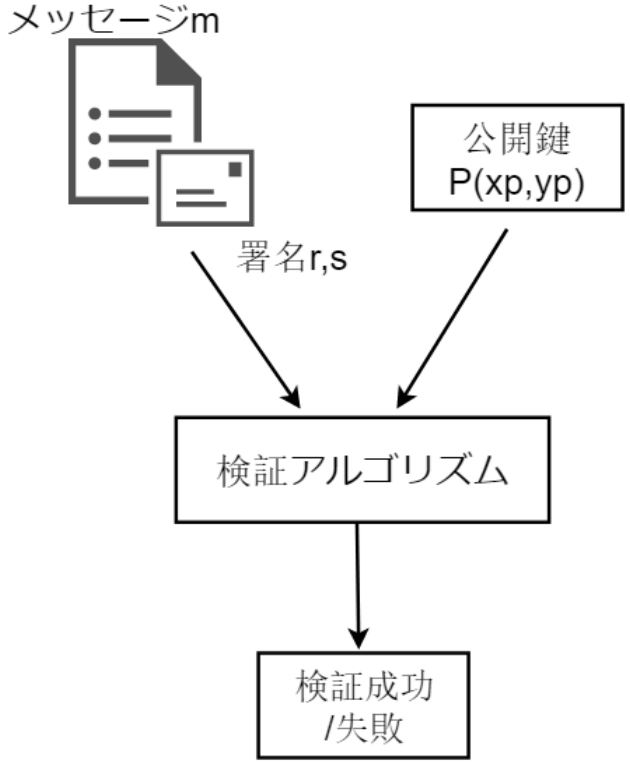
符号化領域

電子署名

紙文書における印鑑や署名に相当するデジタルデータに対するもの



署名



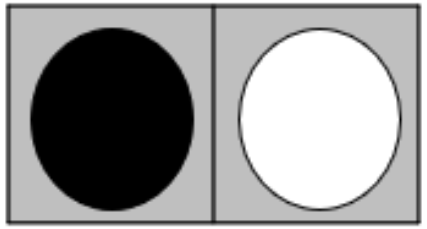
検証

既存研究

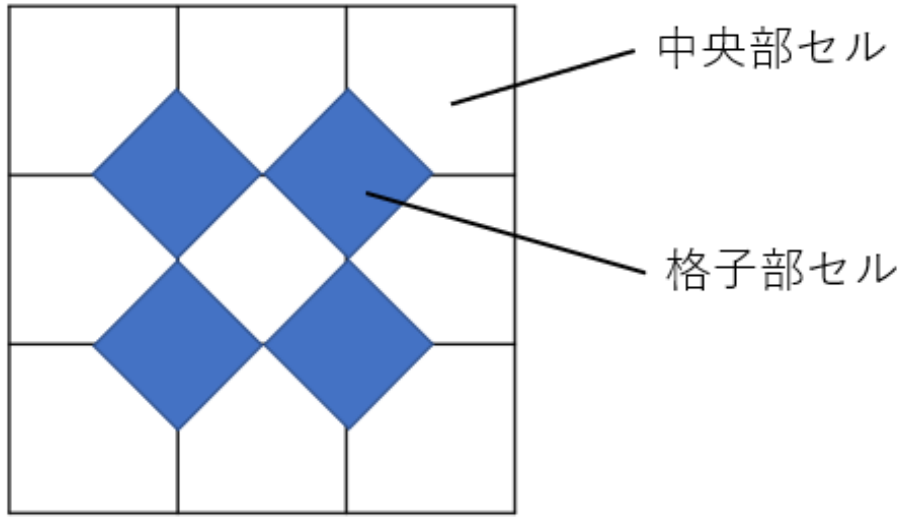
	柏井(2012)	先名(2017)	本研究
暗号化方式	RSA方式	ECDSA方式	ECDSA方式
公開鍵長	2048ビット	160ビット	最小160ビット （任意長可能）
電子署名記憶方式	埋め草領域	誤り訂正部	別空間
課題	電子署名データが大きい ＱＲコードが大きい	誤り訂正能力がなくなる	現実的な環境で評価する

菱形サブセルの提案[3]

・サンプリングとして採用されてないセル周辺の不寄与領域を利用する



不寄与領域
（灰色部分）



中央部セルと格子部セル

[3]寺浦 信之，越前 功，岩村 恵市．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． CSS2019

本研究の概要

・研究目的

ＱＲコードの安全性を高まるため，ＱＲコードに電子署名を埋め込む

・進捗

菱形サブセルを用いる認証可能なＱＲコード作成、識別システム

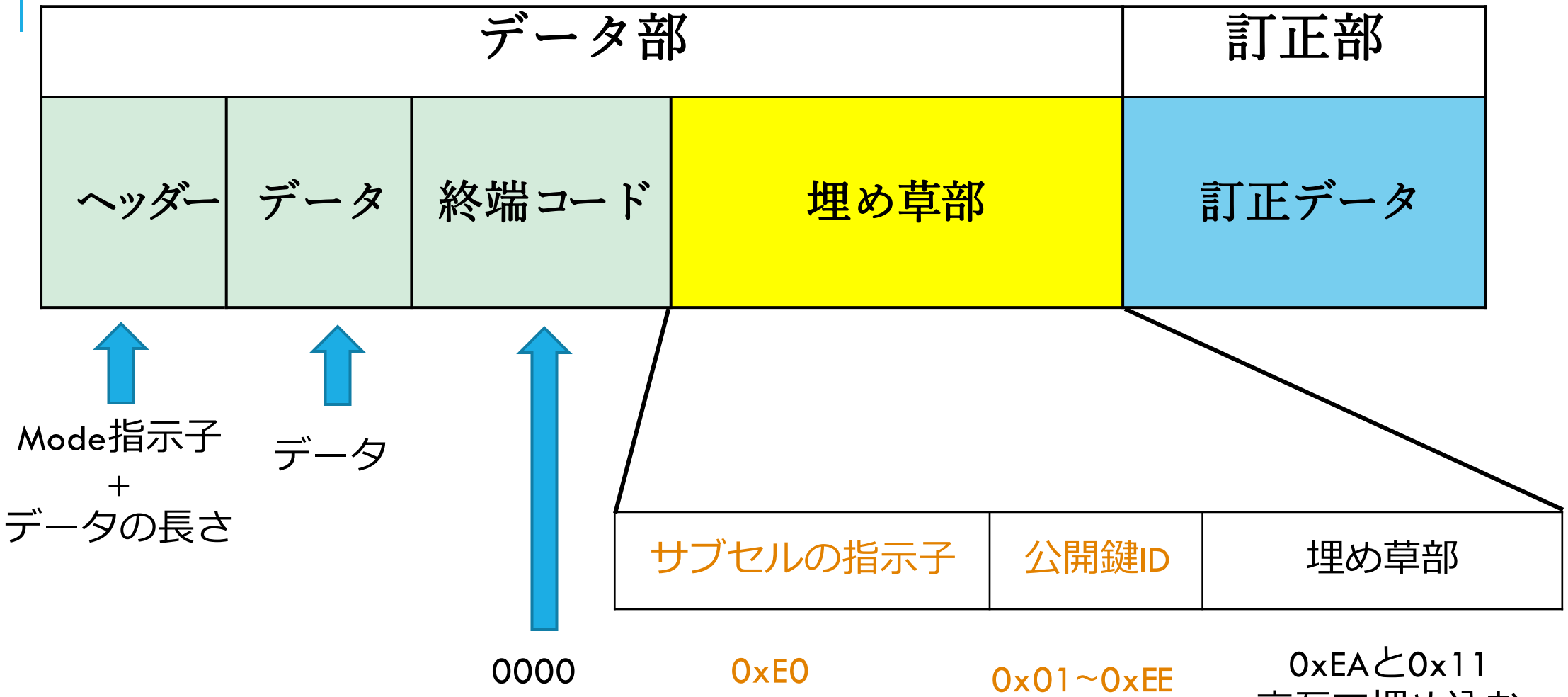
ＱＲコードに対する耐性実験

解決する必要がある課題

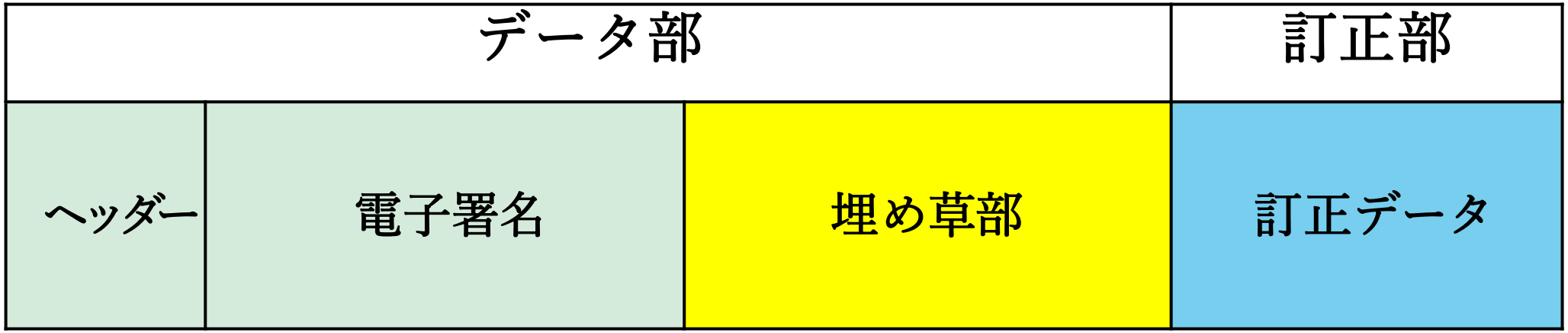
- 署名を埋め込む空間を確保する
- 署名に対する誤り訂正
- データと区別できる区間を作る

これらの三つの問題を解決できる生成システムを説明する.

ＱＲコード中央部セル符号化領域の構成



ＱＲコード格子部セル符号化領域の構成



菱形サブセルを用いるＱＲコードの生成手順

通常のＱＲコードの生成

↓

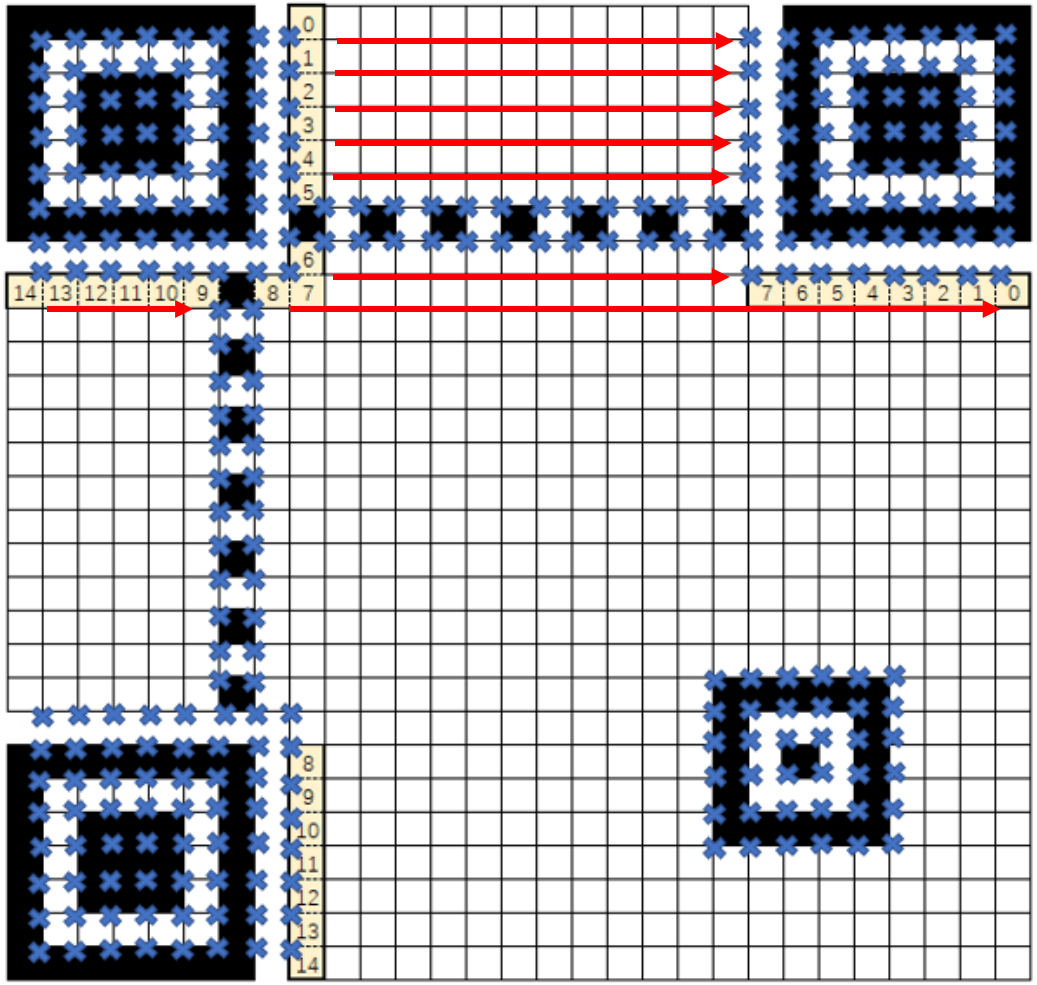
電子署名を生成

↓

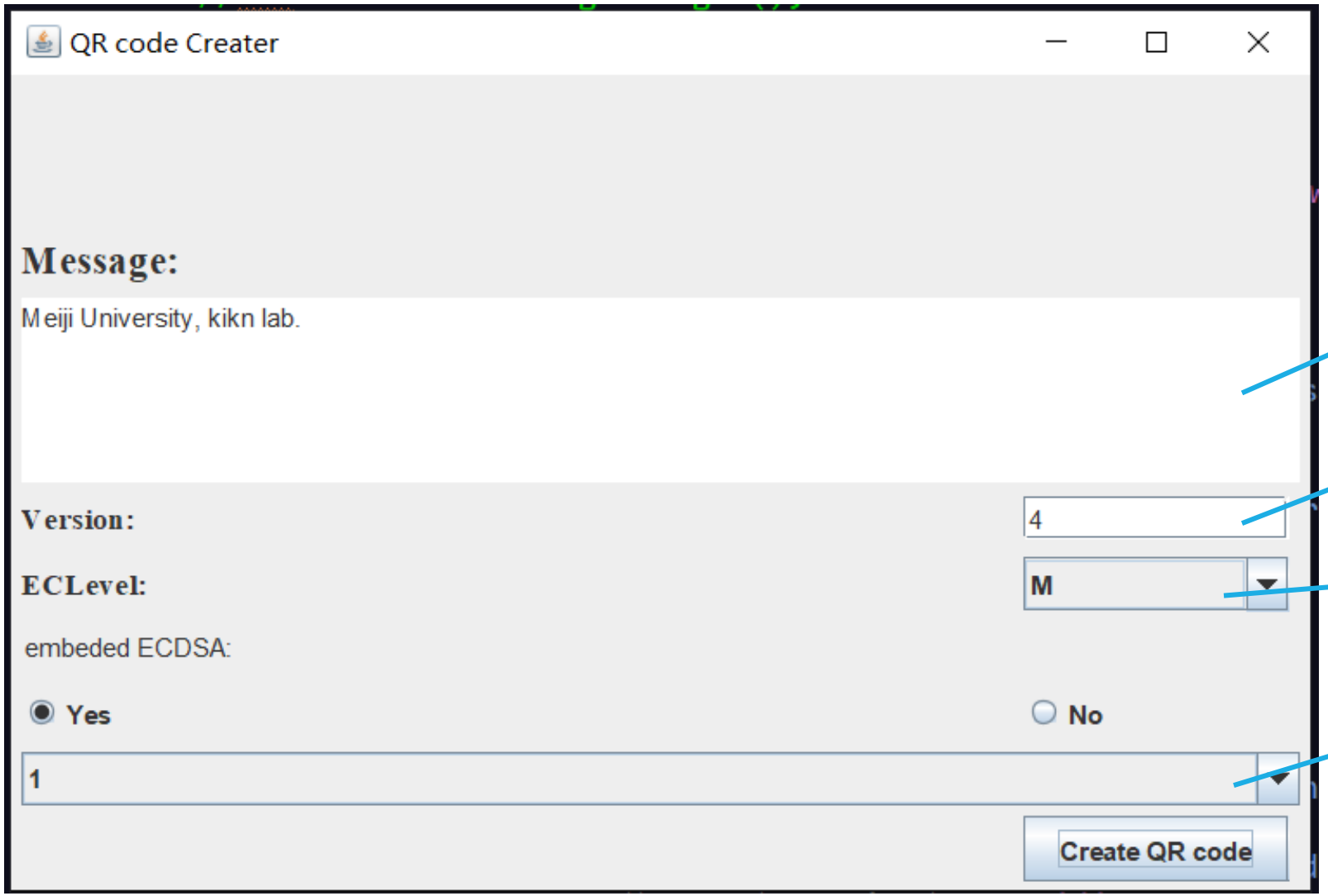
電子署名に対する誤り訂正

↓

左上から順番に電子署名、
誤り訂正符号を埋めこむ



生成ソフト



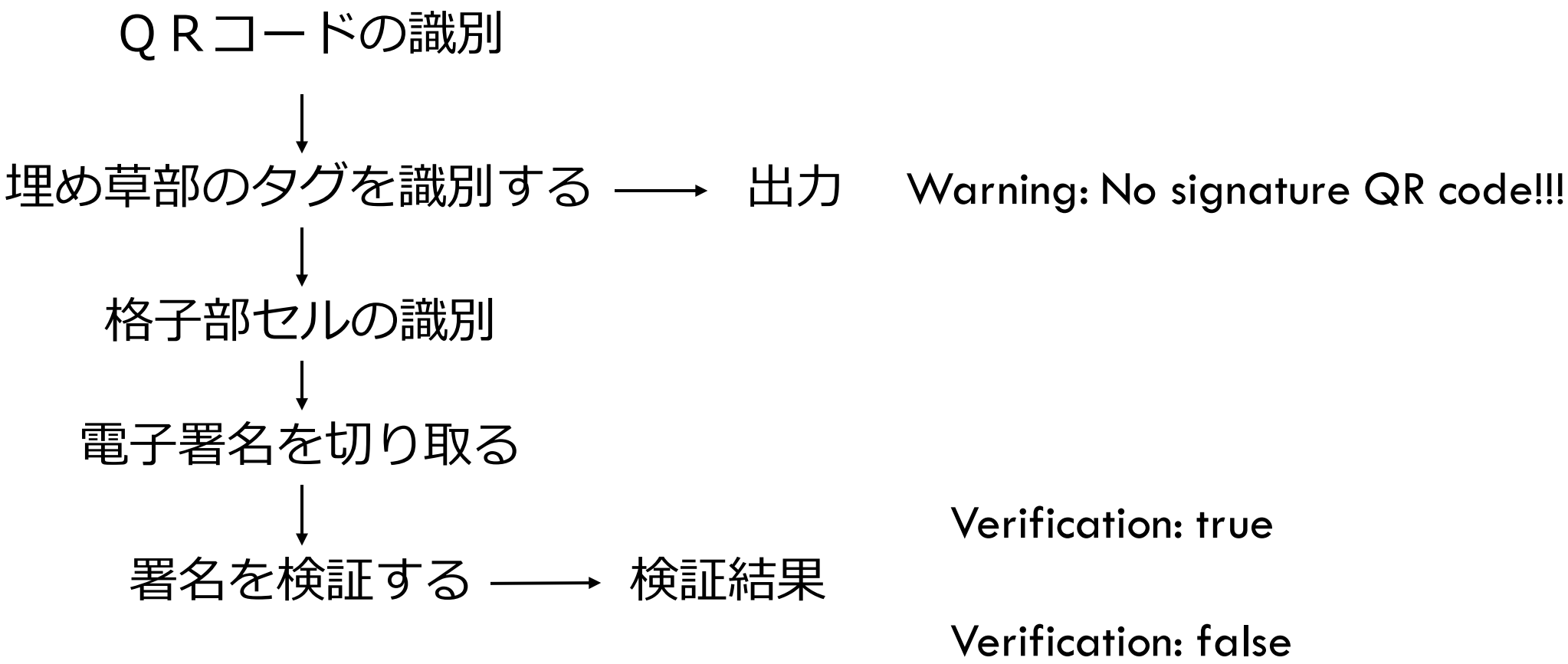
生成ソフトの実行例

生成されたＱＲコードの例

通常のＱＲコード

署名付きなＱＲコード

識別の流れ


ＱＲコードの識別
埋め草部のタグを識別する
出力
Warning: No signature QR code!!!
格子部セルの識別
電子署名を切り取る
署名を検証する
検証結果
Verification: true
Verification: false

識別結果（１）

```
numData is :428
mode is :BYTE
the tag is: 236
bitmatrix resultText is：Meiji University, kikn lab.
bitmatrix RawBytes is：[B@368102c8
bitmatrix NumBits is：440
bitmatrix mark is：0
warning: No signature QR code!!!!!!
```

電子署名なしＱＲコードの読み取り結果例

```
numData is :428
mode is :BYTE
bitmatrix resultText is：Meiji University, kikn lab.
bitmatrix RawBytes is：[B@368102c8
bitmatrix NumBits is：440
bitmatrix mark is：1
There is a signature in QR code's subcell
subcell data:[B@dcf3e99
whole subcell code word is:[B@dcf3e99
the subcell data(signature) is:
 ..XX.... ..X.XX.X ......X. ...X.X.. .XX...XX ....XX.X ...XXX.X .X.X.X.. .XXXXXX. .XXXX.XX .X.X.XXX .X.XX..X .XXXXX.. ..
signature is:[B@75a1cd57
signature ecdsa verification:true
PUBLIC_KEY:MD4wEAYHKoZIzj0CAQYFK4EEAAkDKgAEBI79Kf7Xt1jJElyZkOKabVPsl2gvK4uWrWvInIT7U5S2Z7BYMn9w1Q==
```

電子署名があるＱＲコードの読み取り結果例

識別結果（２）

```
numData is :244
mode is :BYTE
bitmatrix resultText is：Meiji University, kikn lab.
bitmatrix RawBytes is：[B@368102c8
bitmatrix NumBits is：512
bitmatrix mark is：2
There is a signature in QR code's subcell
subcell data:[B@dcf3e99
whole subcell code word is:[B@dcf3e99
the subcell data(signature) is:
 ..XX.... ..X.XX.. ......X. ...X.X.. ...XX..X X.XX.... XXX..XX. .XXXX..X XX..XX.X XXX..... X.X..XX. .X..X.X. X...X.X. .X
signature is:[B@75a1cd57
signature ecdsa verification:false
PUBLIC_KEY:MD4wEAYHKoZIzj0CAQYFK4EEAAkDKgAEBI79Kf7Xt1jJElyZkOKabVPsl2gvK4uWrWvInIT7U5S2Z7BYMn9w1Q==
```

中央部セルデータを改ざんしたＱＲコードの読み取り結果例

耐性実験

菱形サブセルの追加により，ＱＲコード識別に対する影響を検証する

バージョン３のＱＲコードを実験対象とする

実験１：誤り増加の影響実験

実験２：解像度に関する実験

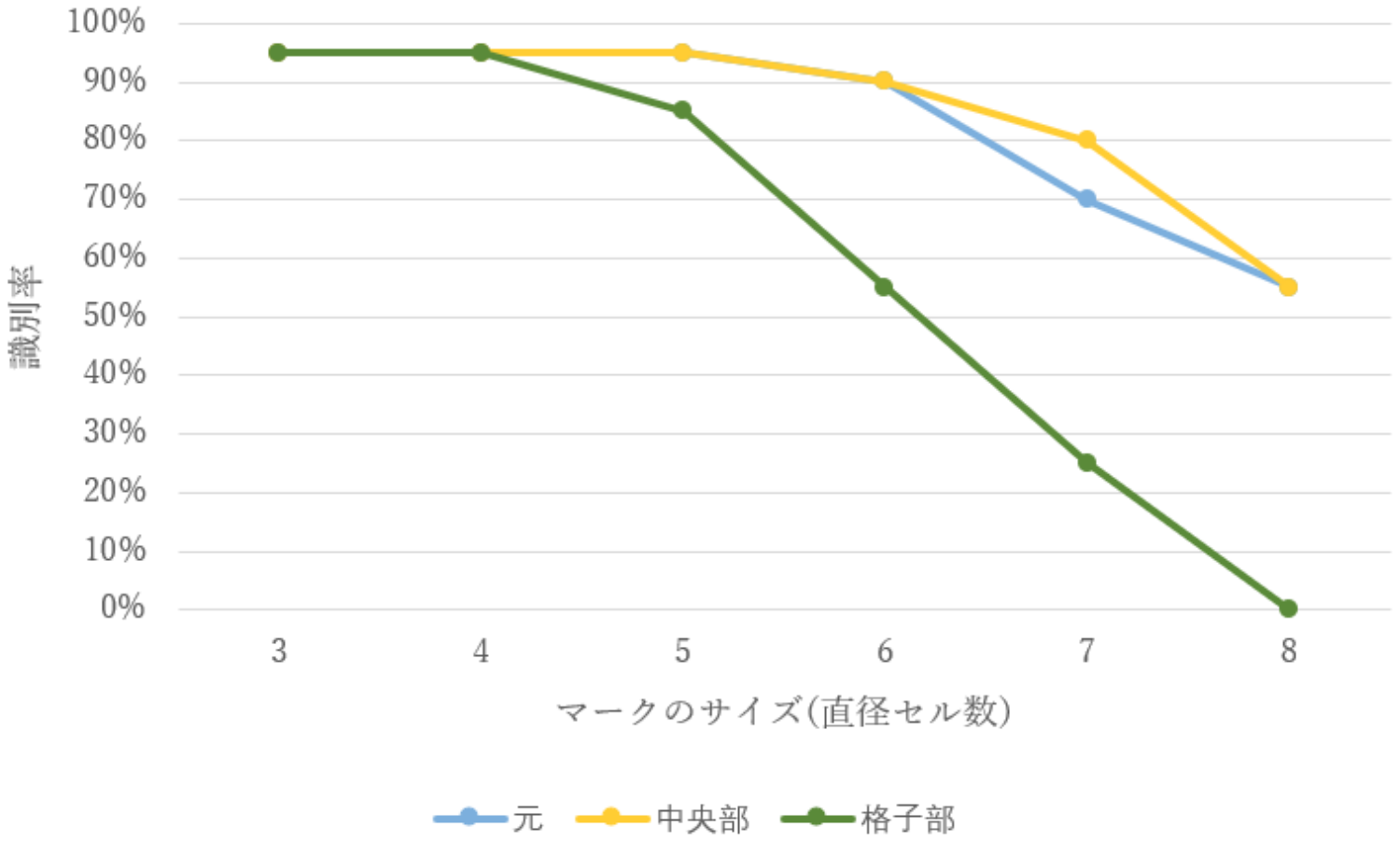
実験１：誤り増加の影響実験

・マークを使い、ＱＲコードの一部を隠す
誤りに対する訂正能力を確認する
・マークのサイズを変え、
ランダムにＱＲコードに貼る
各マークサイズに対して二十回ずつ実験を行う

誤りとして使ったマーク

実験例

実験１　実験結果


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
識別率
3
4
5
6
7
8
マークのサイズ(直径セル数)
元
中央部
格子部

実験２：解像度に関する実験

・解像度が低くなる時，ＱＲコードの識別性能を検証する

・通常のQRコードと菱形サブセルを用いるＱＲコード
　の識別能力を検証する

・ＱＲコードのサイズは800×800ピクセルから下げる
　（800　600　400　300　200　100など）

・各解像度下に，メッセージのサイズを変わり，実験を10回ずつ行った

800×800

400×400

200×200

100×100

60×60

800×800

400×400

200×200

100×100

実験２　実験結果

解像度 （ピクセル）	通常のＱＲコード 識別率(%)	菱形サブセルを用いる ＱＲコード識別率(%)
800×800	100	100
600×600	100	100
400×400	100	100
300×300	100	100
250×250	100	100
200×200	100	100
150×150	100	0
100×100	100	0
80×80	100	0
60×60	0	0

従来のQRコードでは10%までに対し，
菱形サブセルを用いるＱＲコードはもとの解像度の25%までは誤りがなく読み取れる事がわかった.

まとめ

・菱形サブセルによる電子署名を追加したＱＲコードの生成、識別システムを開発した

・菱形サブセルを用いるＱＲコード

中央部セルの読み取りへの影響は生じていなかった

格子部セルは誤りに対する耐性が中央部セルより弱い

・解像度に関する実験では、

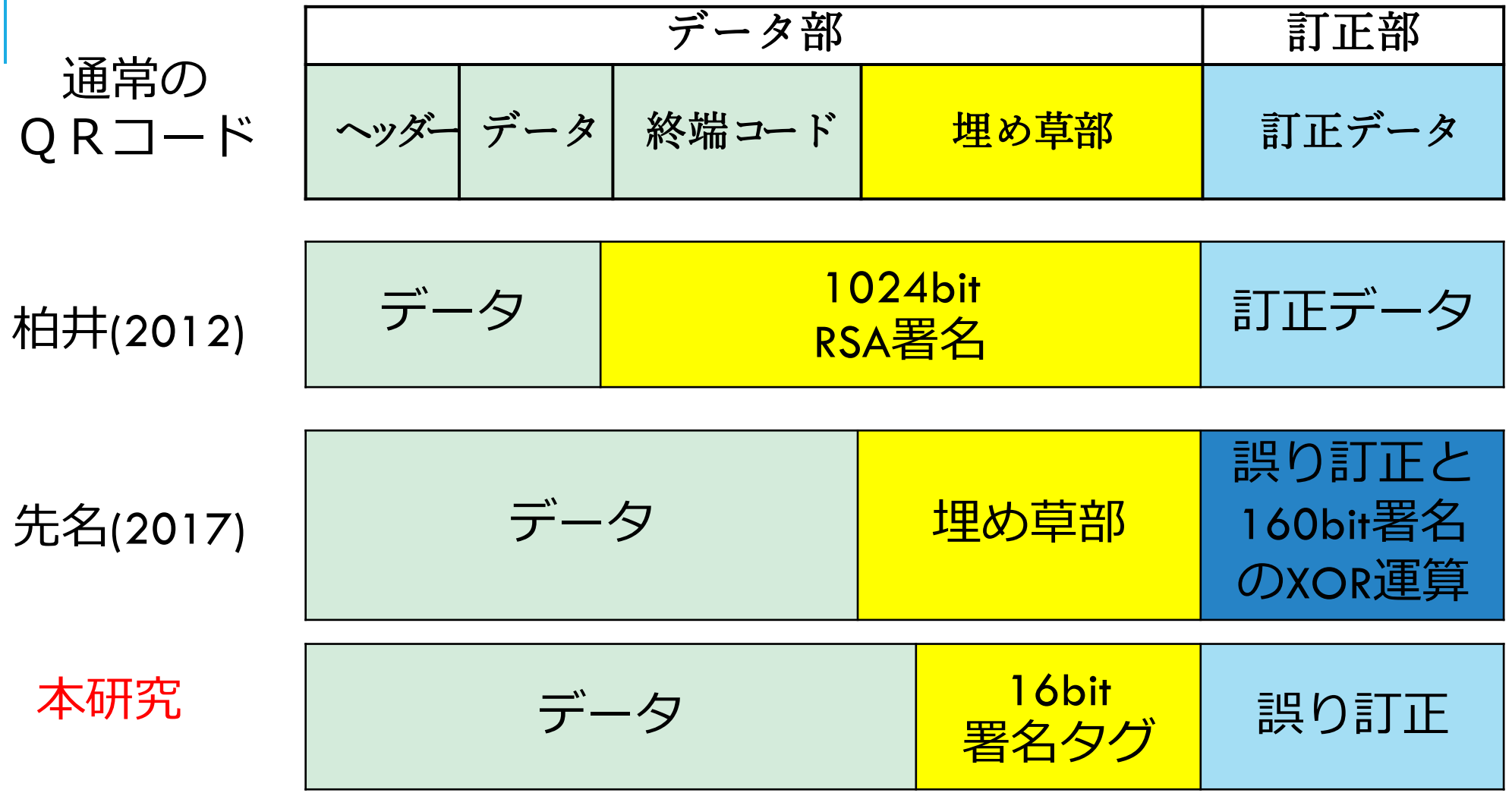
菱形サブセルを用いるＱＲコードはもとの解像度の25%までは誤りがなく読み取れる事がわかった.

・全ての実験は画像を人工的に操作して模擬的に行い、今後はアプリケーションの開発し，より現実的な環境での評価する

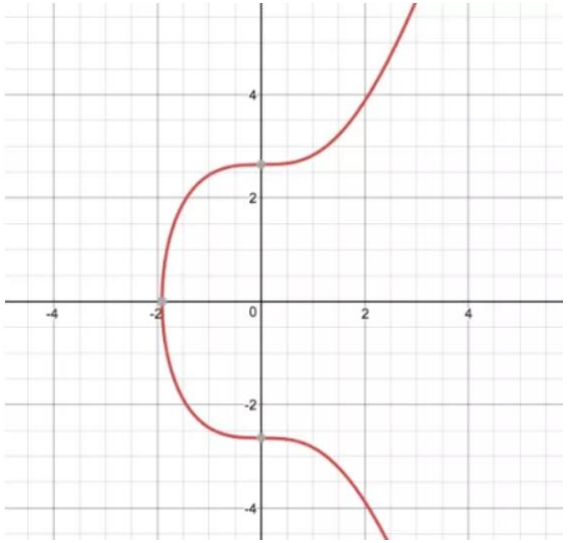
ご清聴ありがとうございました

質疑応答

既存研究


通常の
ＱＲコード
データ部
訂正部
ヘッダー
データ
終端コード
埋め草部
訂正データ
柏井(2012)
データ
1024bit
RSA署名
訂正データ
先名(2017)
データ
埋め草部
誤り訂正と
160bit署名
のXOR運算
本研究
データ
16bit
署名タグ
誤り訂正

ECDSA(ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM)



ECDSAは楕円曲線に基づく有限体において

定義されているデジタル署名である.

一般的に，楕円曲線は以下のような方程式で表される.

$$y^2 = x^3 + ax + b$$

DSA（Digital Signature Algorithm ）は離散対数問題の困難性に基づく電子署名方式である.

電子署名の仕様

160bitの署名を例として

0x30 + LEN1 + 0x02 + LEN2 + 00 (optional) + r + 0x02 + LEN3 + 00(optional) + s

302e021500b7cdd2b24abf3f48e612d39fbd651b215a26b3e3021500a19c672a73cc73fec77a14c5481c426e81b678a5

(20btyes) (20btyes)

LEN3=0x00(optional) + s

LEN2=0x00(optional) + r

LEN1=LEN2+LEN3+4

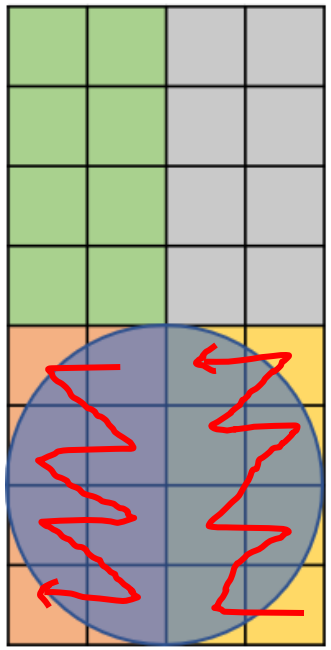
総LEN：46～48　bytes

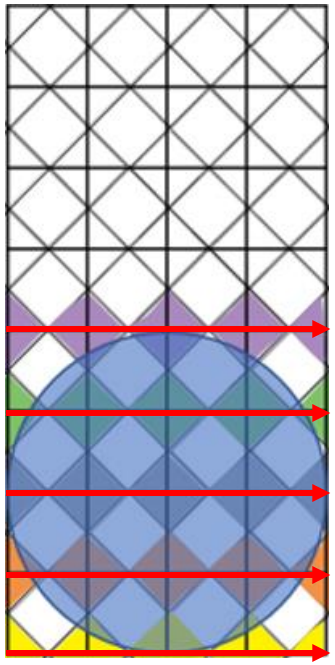
※ r とsの一番目のbyteは0x80より大きな時0x00を付ける。

実験１　菱形サブセルの識別率が低い原因

・誤りに影響される格子部セルの数は中央部セルより多い

・菱形サブセルを埋め込む順番と関係がある





QRコードの仕様

・型番：
1型（21 × 21）～
40型（ 177 × 177 ）

・誤り訂正：
復元可能な損傷割合

・1コード＝8ビット

バージョン（サイズ）	誤り訂正レベル				コード語数
	L (7%)	M (15%)	Q (25%)	H (30%)	
1 (21x21)	17	14	11	7	26
2 (25x25)	32	26	20	14	44
3 (29x29)	53	42	32	24	70
4 (33x33)	78	62	46	34	100
5 (37x37)	106	84	60	44	134
6 (41x41)	134	106	74	58	172
7 (45x45)	154	122	86	64	196

※

V1

V2

V3

V4

V5

菱形サブセルを用いる3-L型ＱＲコード

６-Ｌ型ＱＲコード

解像度 （ピクセル）	菱形サブセルを用いる 3-L型ＱＲコード識別率(%)	6-L型ＱＲコード識別率(%)
800×800	100	100
600×600	100	100
400×400	100	100
300×300	100	0
250×250	100	0
200×200	100	0
150×150	0	0
100×100	0	0
80×80	0	0
60×60	0	0

格子部をいれることで、どれくらいデータが増える？

（byte数）

ＱＲコードの型番	通常な ＱＲコード	菱形サブセルを用いる ＱＲコード
3-L	55	53+48
4-L	80	78+77
4-H	64	62+63
5-L	108	106+105
5-H	86	84+83
5-Q	64	62+59
6-L	136	134+135