
SBA
Research

Error-Correcting Codes as Source for Decoding Ambiguity

Adrian Dabrowski, Isao Echizen, Edgar Weippl

adabrowski@sba-research.org

2015-05-21

COMET
Competence Centers for Excellent Technologies

SBA Research

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfw Bundesministerium für Wissenschaft, Forschung und Wirtschaft
FFG
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds

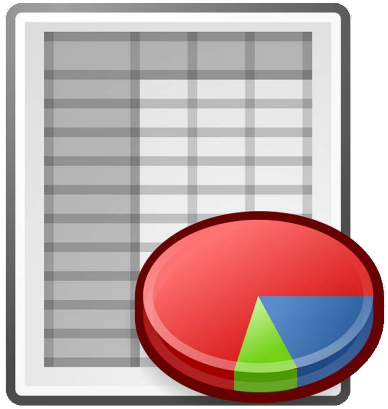
Preface

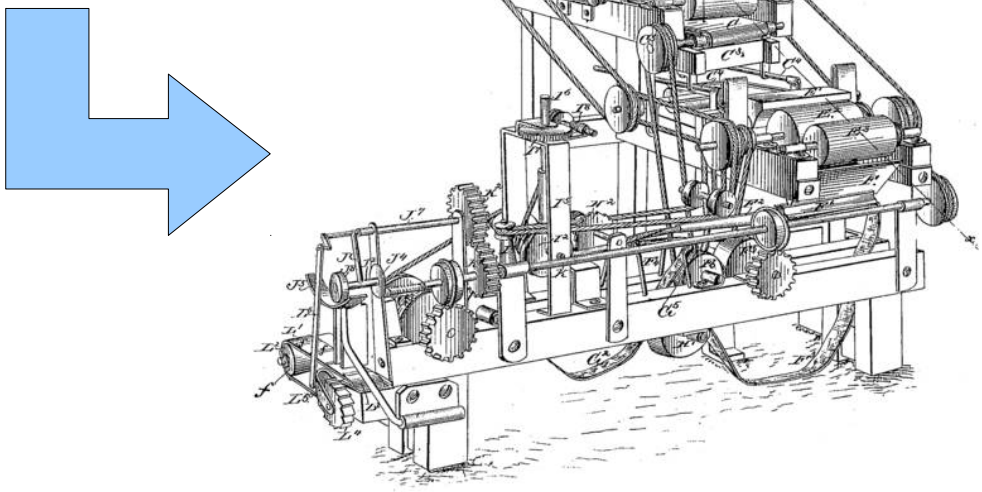
- File format
  == data format
  == protocol
  == language
- File
  == transmission
  == data stream
  == packet(s)

SBA Research

Input path

```
25 50 44 46 2d 31 2e 35
38 20 30 20 6f 62 6a 0a
74 68 20 34 37 32 34 20
69 6c 74 65 72 20 2f 46
64 65 0a 3e 3e 0a 73 74
3b d9 72 e3 46 92 ef fe
f7 31 f3 62 59 7d 44 b7
3f 80 64 89 c4 34 09 d0
50 00 41 49 f6 6c 6c c4
ca 4c 79 57 db 2b ef ea
```

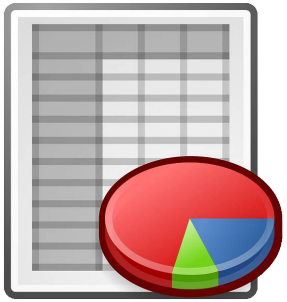


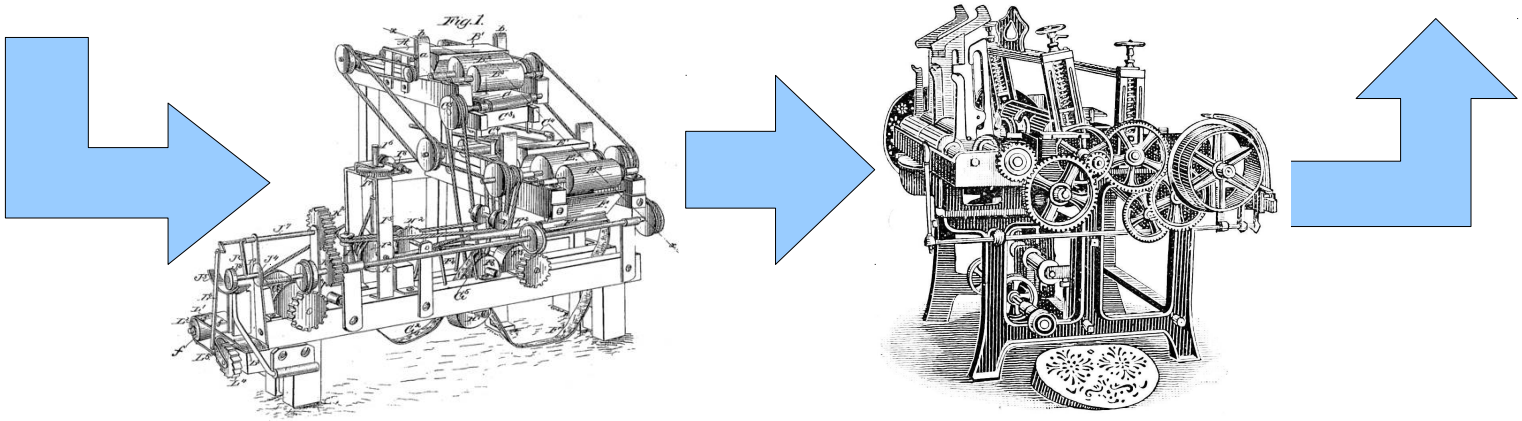


SBA Research

Input path

```
25 50 44 46 2d 31 2e 35
38 20 30 20 6f 62 6a 0a
74 68 20 34 37 32 34 20
69 6c 74 65 72 20 2f 46
64 65 0a 3e 3e 0a 73 74
3b d9 72 e3 46 92 ef fe
f7 31 f3 62 59 7d 44 b7
3f 80 64 89 c4 34 09 d0
50 00 41 49 f6 6c 6c c4
ca 4c 79 57 db 2b ef ea
```





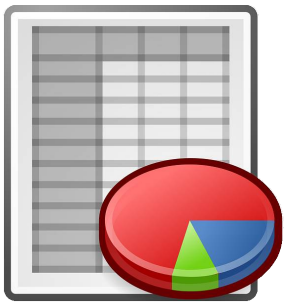
SBA Research

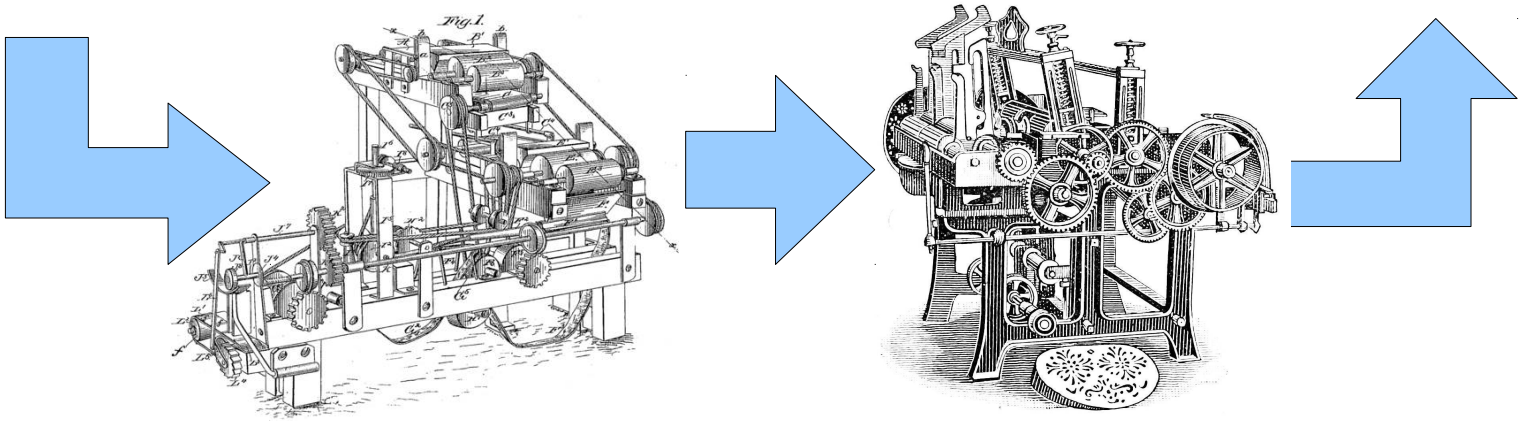
Input path

```
25 50 44 46 2d 31 2e 35
38 20 30 20 6f 62 6a 0a
74 68 20 34 37 32 34 20
69 6c 74 65 72 20 2f 46
64 65 0a 3e 3e 0a 73 74
3b d9 72 e3 46 92 ef fe
f7 31 f3 62 59 7d 44 b7
3f 80 64 89 c4 34 09 d0
50 00 41 49 f6 6c 6c c4
ca 4c 79 57 db 2b ef ea
```

e.g.

- Synchronizer
- Layered Data
- Compressed Data
- Error Correction
- Container Formats

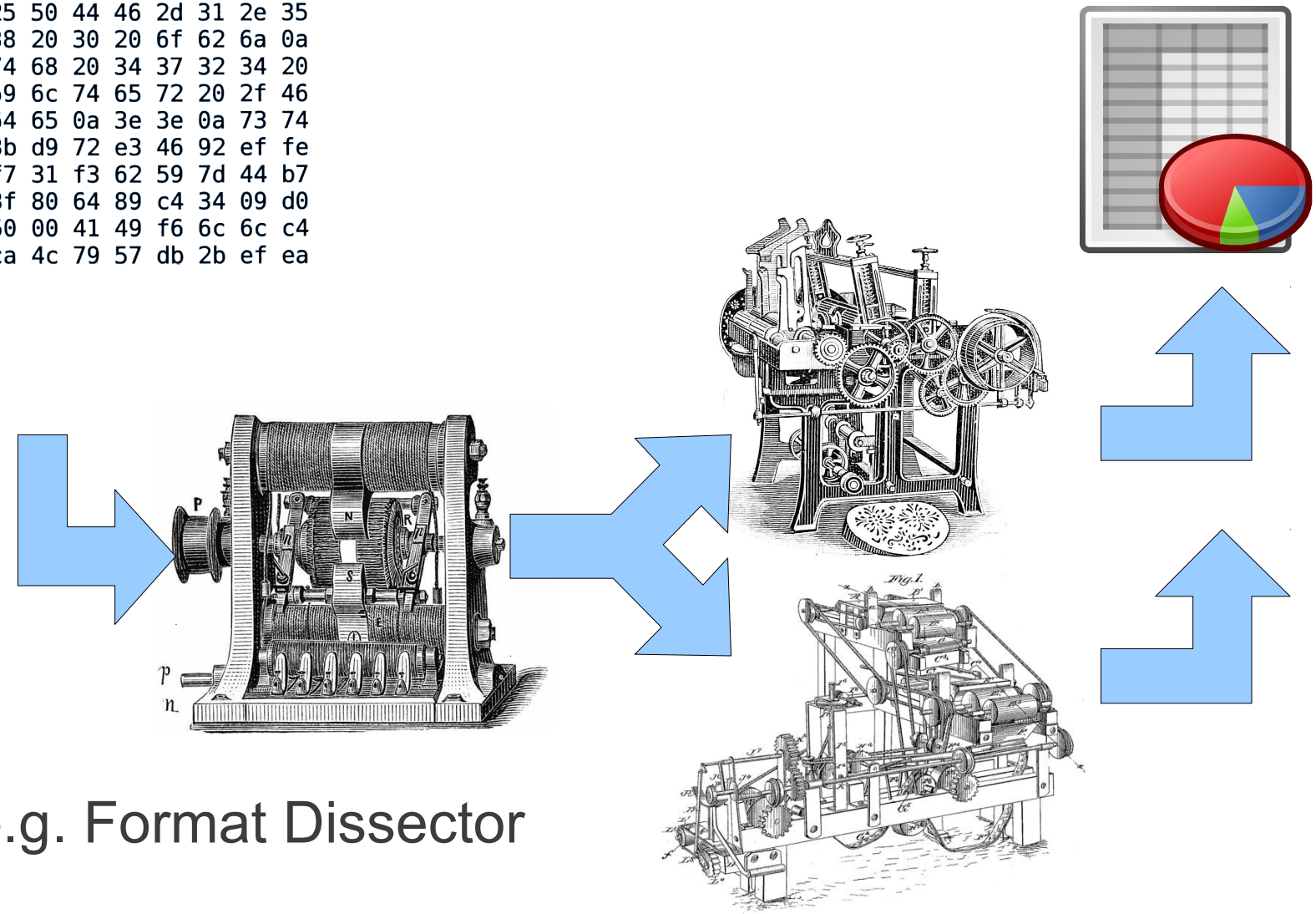




SBA Research

Input path

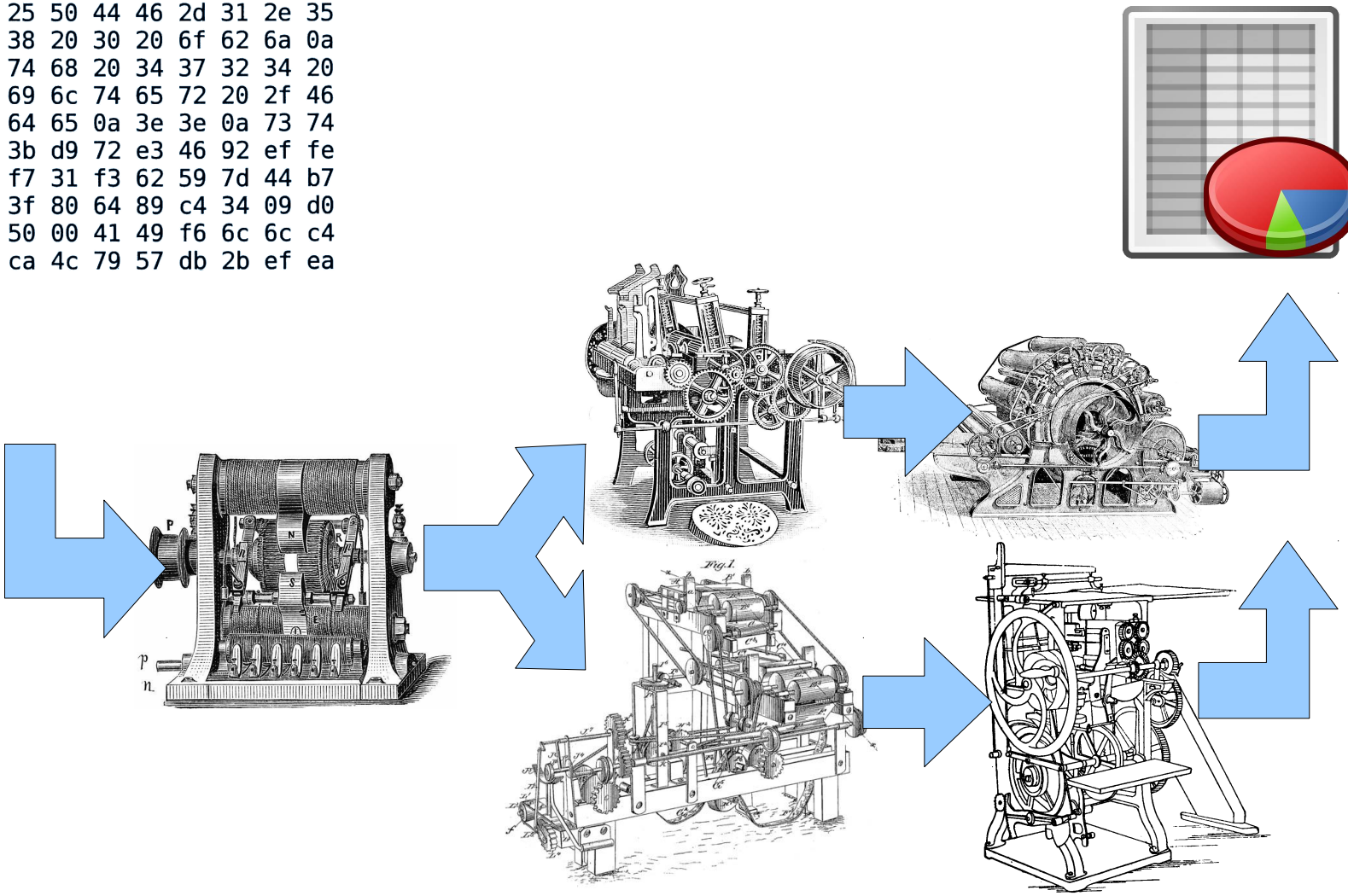
```
25 50 44 46 2d 31 2e 35
38 20 30 20 6f 62 6a 0a
74 68 20 34 37 32 34 20
69 6c 74 65 72 20 2f 46
64 65 0a 3e 3e 0a 73 74
3b d9 72 e3 46 92 ef fe
f7 31 f3 62 59 7d 44 b7
3f 80 64 89 c4 34 09 d0
50 00 41 49 f6 6c 6c c4
ca 4c 79 57 db 2b ef ea
```



e.g. Format Dissector

Input path

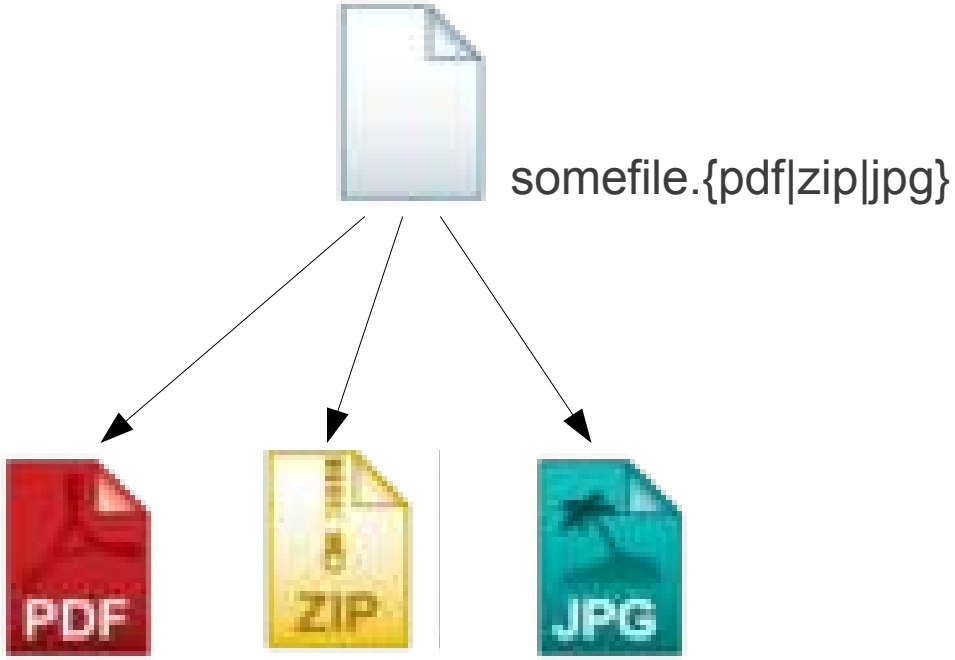
```
25 50 44 46 2d 31 2e 35
38 20 30 20 6f 62 6a 0a
74 68 20 34 37 32 34 20
69 6c 74 65 72 20 2f 46
64 65 0a 3e 3e 0a 73 74
3b d9 72 e3 46 92 ef fe
f7 31 f3 62 59 7d 44 b7
3f 80 64 89 c4 34 09 d0
50 00 41 49 f6 6c 6c c4
ca 4c 79 57 db 2b ef ea
```



SBA Research

Binary Polyglots

- One file



- Valid as **PDF** **ZIP** **JPEG** simultaneously
- e.g. new editions of POC||GTFO

Ange Albertini, http://code.google.com/p/corkami/#Binary_files

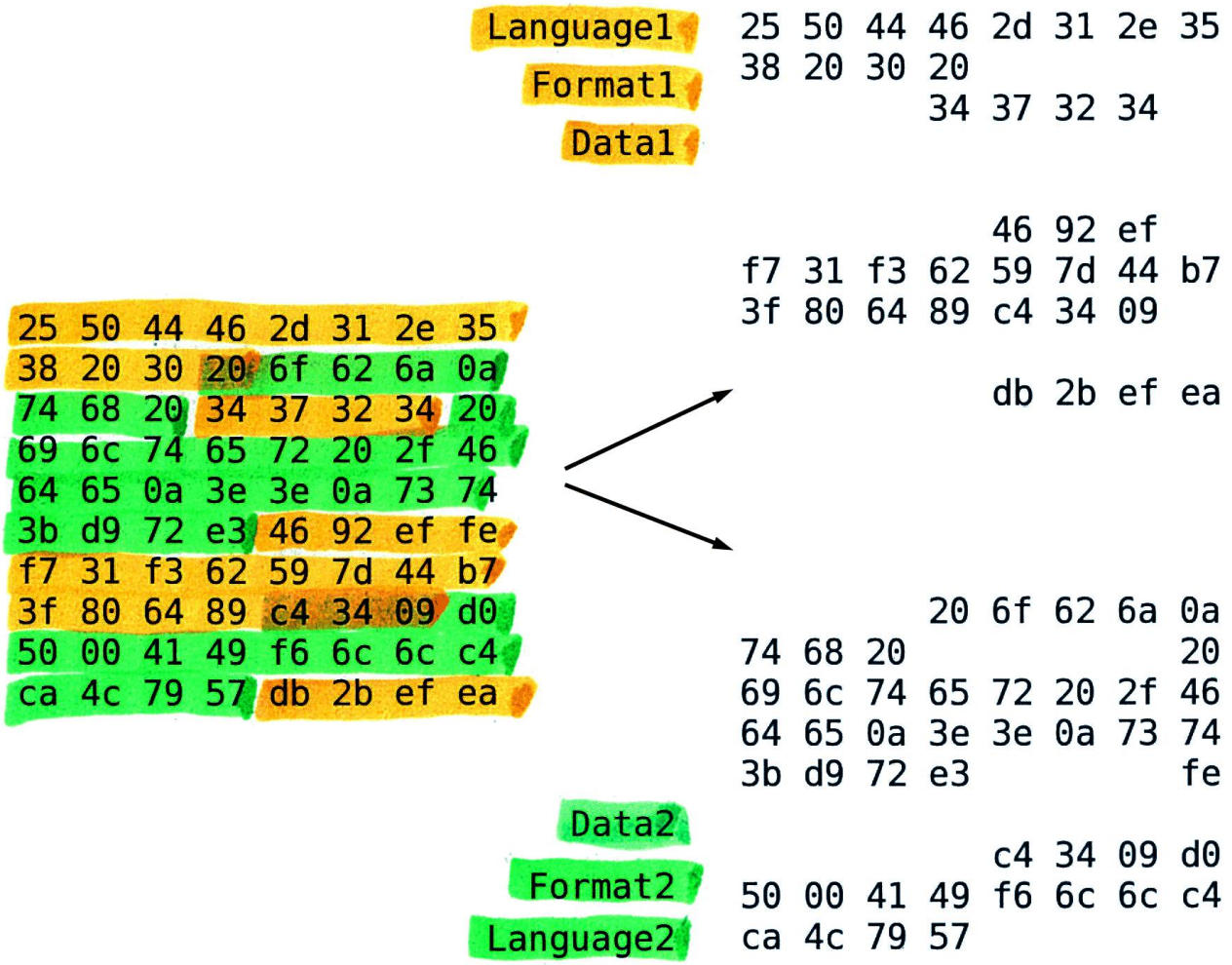
SBA Research

Polyglot

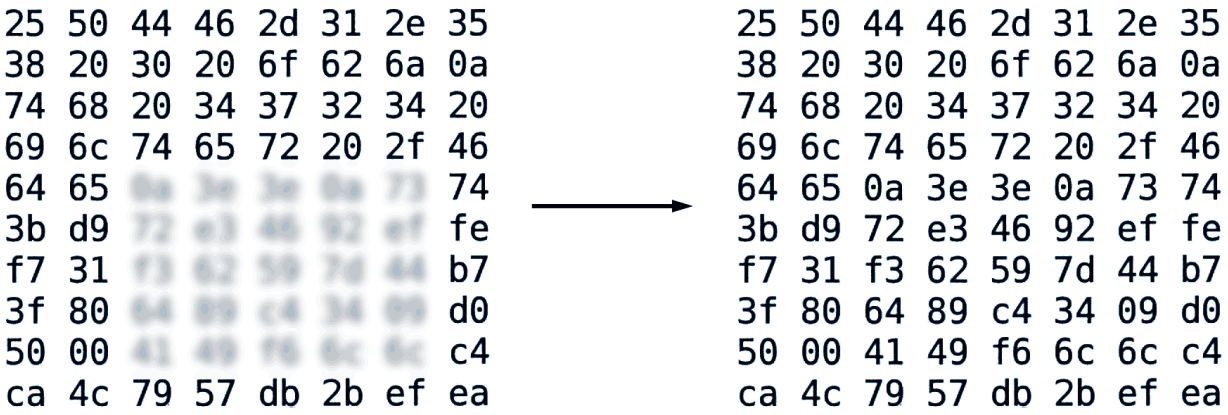
```
25 50 44 46 2d 31 2e 35
38 20 30 20 6f 62 6a 0a
74 68 20 34 37 32 34 20
69 6c 74 65 72 20 2f 46
64 65 0a 3e 3e 0a 73 74
3b d9 72 e3 46 92 ef fe
f7 31 f3 62 59 7d 44 b7
3f 80 64 89 c4 34 09 d0
50 00 41 49 f6 6c 6c c4
ca 4c 79 57 db 2b ef ea
```

SBA Research

Polyglot


Language1
Format1
Data1
Data2
Format2
Language2
25 50 44 46 2d 31 2e 35
38 20 30 20 6f 62 6a 0a
74 68 20 34 37 32 34 20
69 6c 74 65 72 20 2f 46
64 65 0a 3e 3e 0a 73 74
3b d9 72 e3 46 92 ef fe
f7 31 f3 62 59 7d 44 b7
3f 80 64 89 c4 34 09 d0
50 00 41 49 f6 6c 6c c4
ca 4c 79 57 db 2b ef ea
25 50 44 46 2d 31 2e 35
38 20 30 20
34 37 32 34
46 92 ef
f7 31 f3 62 59 7d 44 b7
3f 80 64 89 c4 34 09
db 2b ef ea
20 6f 62 6a 0a
74 68 20 20
69 6c 74 65 72 20 2f 46
64 65 0a 3e 3e 0a 73 74
3b d9 72 e3 fe
c4 34 09 d0
50 00 41 49 f6 6c 6c c4
ca 4c 79 57

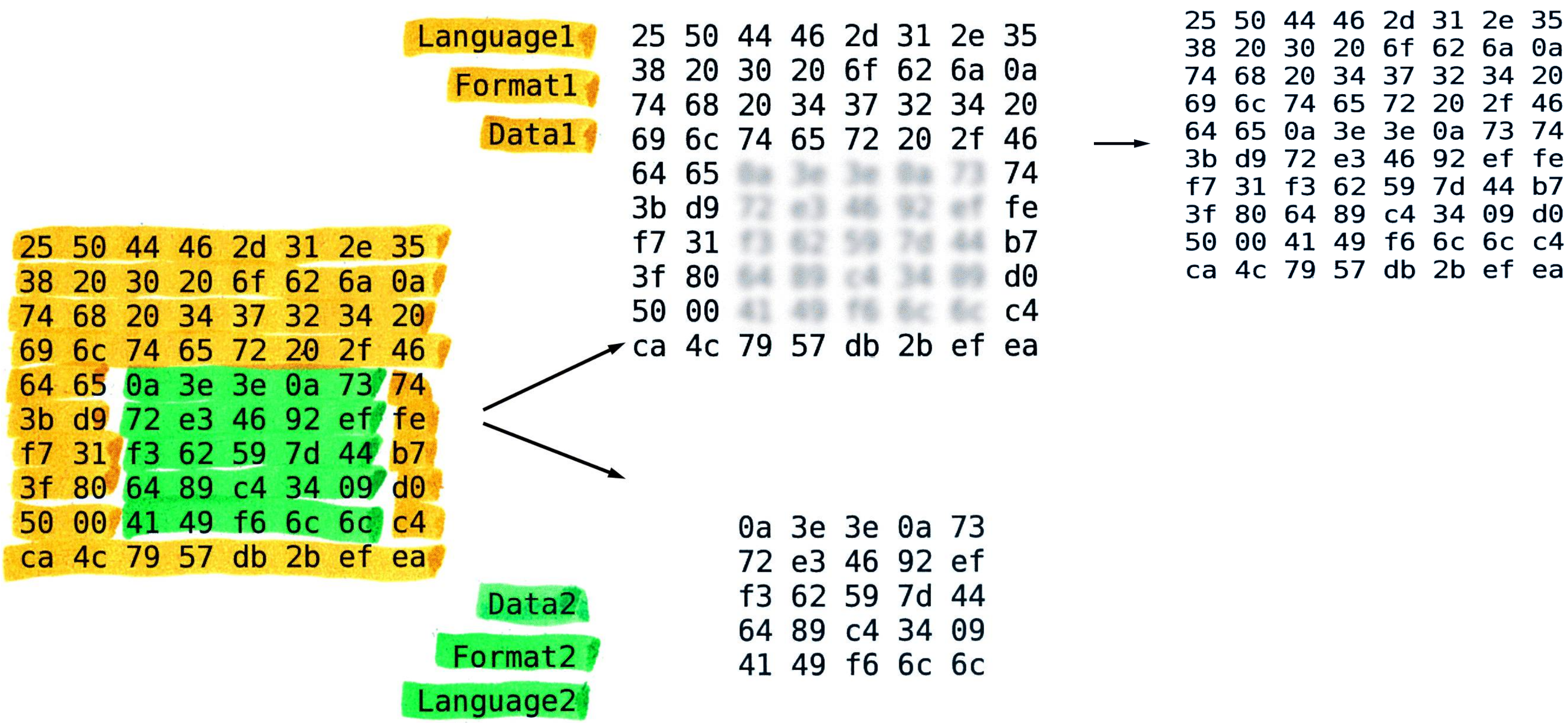
Error Correction



- Data transmission
  - Digital Radio Broadcast (DAB), Digital Video Broadcast (DVB-T, DVB-S, DVB-C)
  - Phone Networks (GSM, UMTS, LTE, Tetra)
- Storage
  - Tapes, HDD, Arrays, Flash, Cloud Storage, Server RAM
  - Barcodes

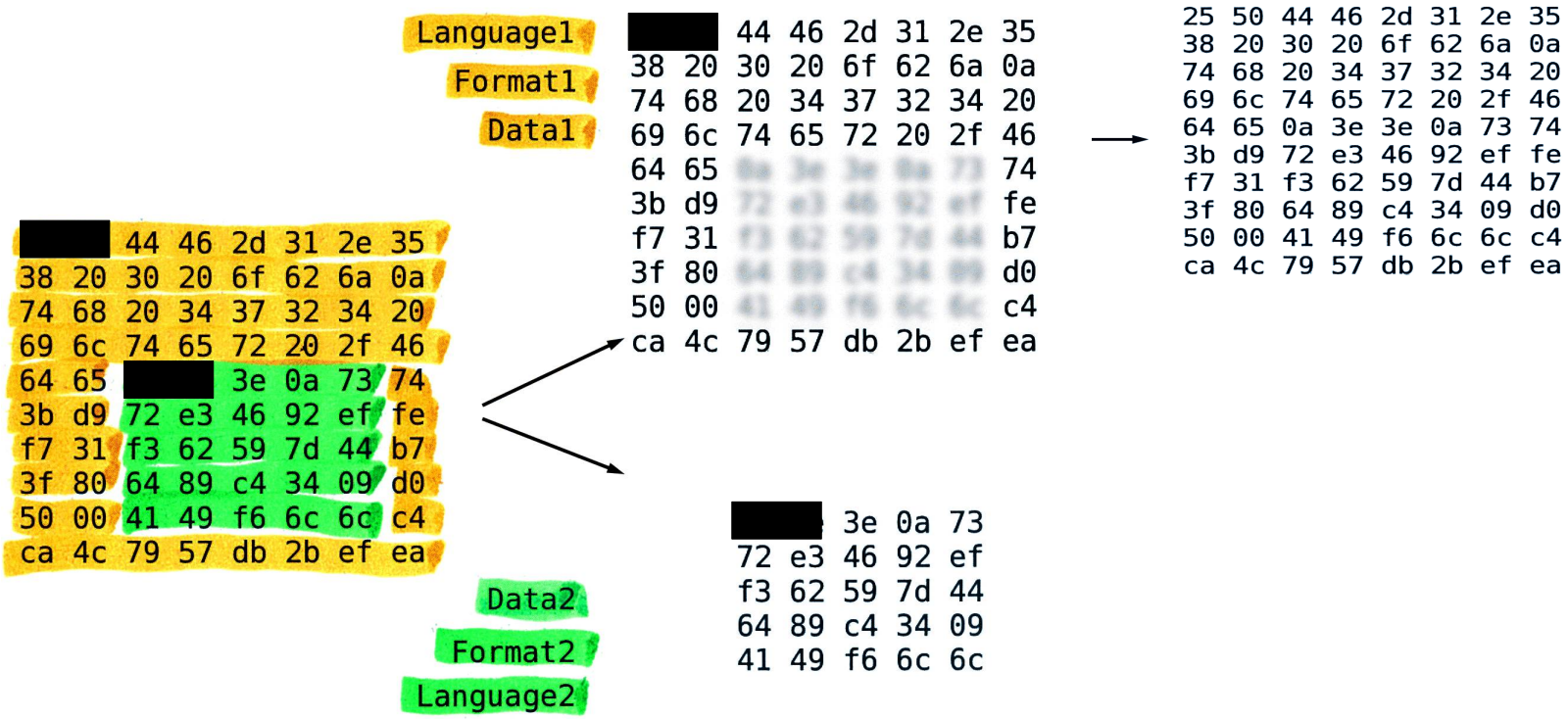
SBA Research

Packet in Packet – via ECC

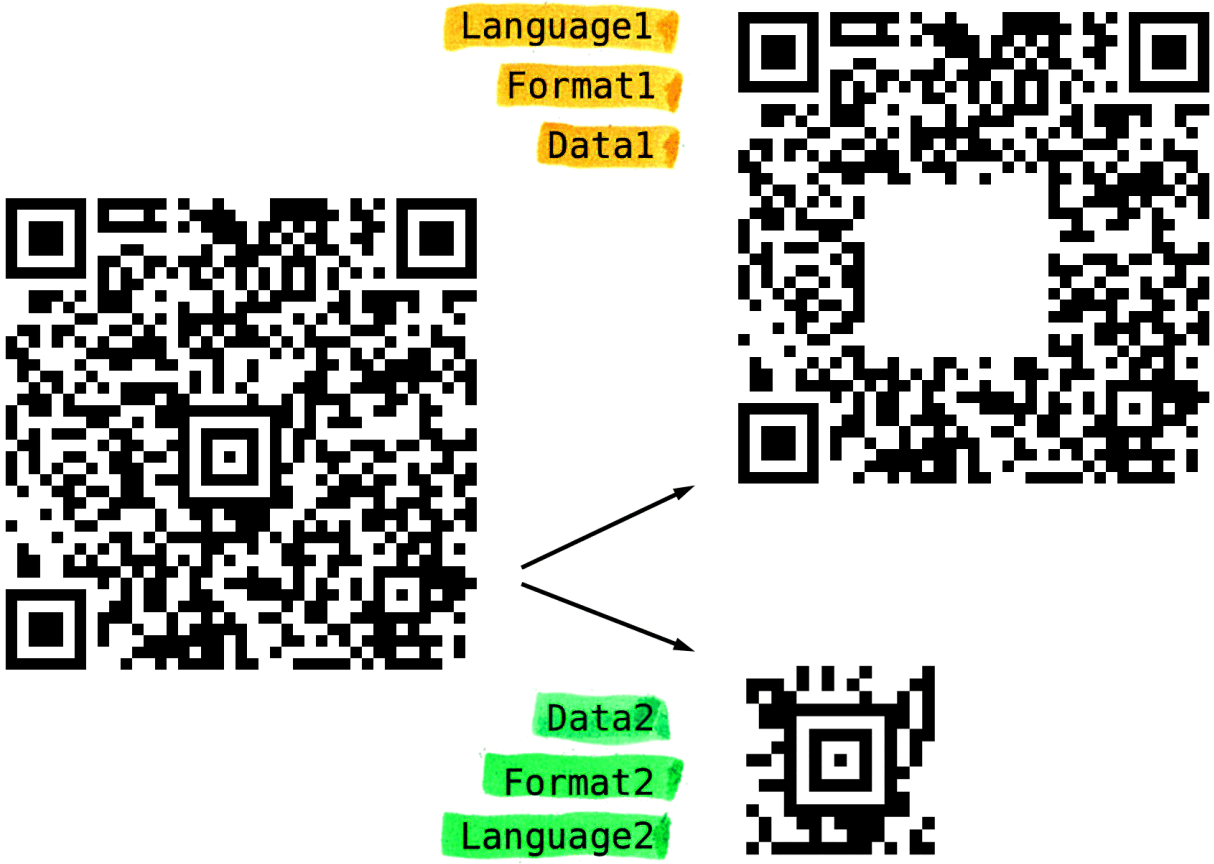


SBA Research

Packet in Packet – via ECC

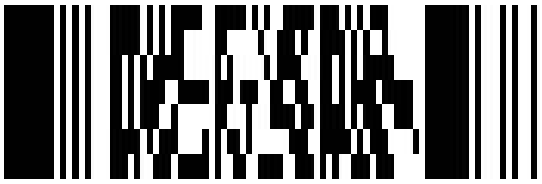


Application: Barcodes



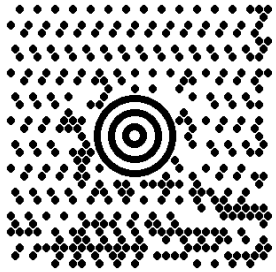
SBA Research

(some) 2D Barcodes

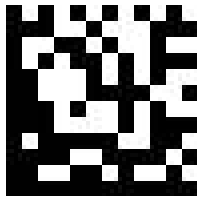


PDF417

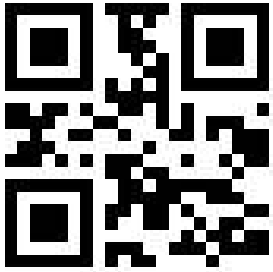
Aztech



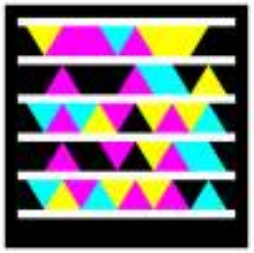
Maxicode



Data Matrix



Quick Response Code



Microsoft Tag
(High Capacity Color Barcode)

3-DI

Shotcode

SBA Research

Testing

OS/Type	Name	QR	Data Matrix	Aztec	Auto-load URLs
iPhone	NeoReader [21]	✓	✓	✓	✓
	Qrafter [16]	✓	✓	✓	✗
	i-nigma [4]	✓	✓	✗	✗
	QR Code Reader and Scanner [27]	✓	✓	✓	✓
	ScanLife [25]	✓	✓	✗	✗
Android	ZXing Barcode Reader [31]	✓	✓	✗	(✗)[1]
	UberScanner [30]	✓	✓	✓	✗
	ScanLife [26]	✓	✓	✗	✓
	i-nigma [5]	✓	✓	✗	✗
	AT&T Code Scanner [9]	✓	✓	✗	✓
	NeoReader [22]	✓	✓	✓	✗
	ShopSavvy [28]	✓	✓	✗	✓
Handheld	Symbol DS6708 [13]	✓	✓	✓	–

SBA Research

Some examples: Aztec

App/Device	Outer	Inner
NeoReader	✓	✓pref.
Qrafter	✗	✗
i-nigma	✓	–
QR Code R.S.	✓	✗
ScanLife	✓	–
ZXing B.S.	✓	–
UberScanner	✓	✓
ScanLife	✓	–
i-nigma	✓	–
AT&T Code S.	✓	–
NeoReader	✓	✓
ShopSavvy	✓	–
DS6708	✓	✓

SBA Research

DM in QR

App/Device	Outer	Inner
NeoReader	✓	✓
Qrafter	✓	✗
i-nigma	✓	✗
QR Code R.S.	✓	✗
ScanLife	✓	✗
ZXing B.S.	✓	✗
UberScanner	✓	✗
ScanLife	✓	✗
i-nigma	(✓)	✗
AT&T Code S.	✓	✗
NeoReader	✓	✓
ShopSavvy	✓	✗
DS6708	✓	✗

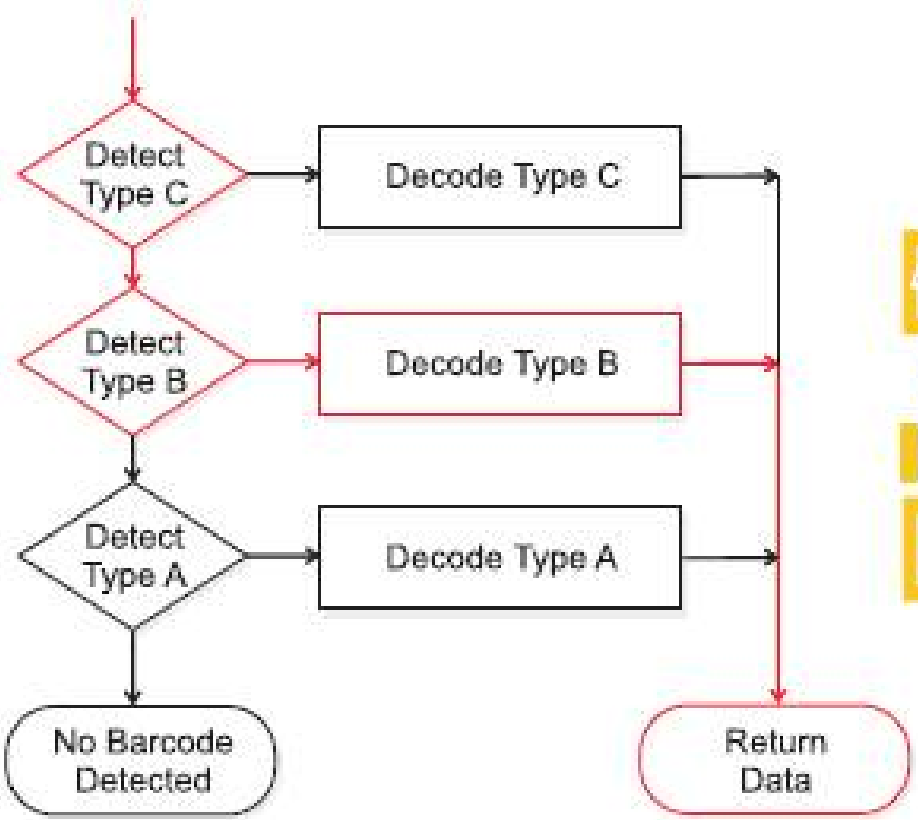
App/Device	Outer	Inner
NeoReader	✗	✓
Qrafter	✓	✓
i-nigma	✓	✓
QR Code R.S.	✓	✗
ScanLife	✓pref.	✓
ZXing B.S.	✓	✓
UberScanner	✓	✓
ScanLife	✓	(✓swipe)
i-nigma	✓	✓
AT&T Code S.	✓	(✓swipe)
NeoReader	✓	✓
ShopSavvy	✓	✓
DS6708	✓	✓

QR in QR

App/Device	Outer	Inner
NeoReader	✓	✗
Qrafter	✗	✗
i-nigma	✓	✓
QR Code R.S.	✗	✗
ScanLife	(✓rot.)	✓
ZXing B.S.	✗	(✓swipe)
UberScanner	✗	(✓swipe)
ScanLife	✗	✗
i-nigma	✓	✗
AT&T Code S.	✗	✗
NeoReader	✓	✗
ShopSavvy	(✓)	✗
DS6708	✓	✓pref.

Many more examples in:
Dabrowski et al. “Barcode-in-Barcode Inception”

Decoding sequence



SBA Research

QR: Only harmless fun?

- 2012: USSD-Codes in Tel:-URLs encoded in Barcodes could wipe a phone.
- Generate Premium-Rate SMS
- URLs can trigger exploits in Web-Browser, Renderer, OS, code Injection, ...
- Used for financial transactions
  - Paypal & Bitcoin

SBA Research

Countermeasures for QR

- Stringent decoding order
  - Root cause of decoding ambiguity
- Present user a visual excerpt
- Notification of all codes found
- Detect & display alien data in barcode
- Do not automatically retrieve & display target URL
- Only decode, what you are looking for

SBA Research

Generic Countermeasures

- Both transmissions are standard compliant!
- Application specific:
  - Drop ambiguities – but need to detect!
  - Choose higher data density
- No easy way – any heuristic (aka guessing) is a risc

SBA Research

Wrap Up

- ECC used in many applications
  - Radio, Broadcast, Storage, ...
- Can be used to include alternative data (streams)
  - Implementation specific / probabilistic
- Any ambiguity is insecurity
- Detecting (in general case) is not easy

SBA Research

Error-Correcting Codes as Source for Decoding Ambiguity

Adrian Dabrowski, Isao Echizen, Edgar Weippl

adabrowski@sba-research.org

2015-05-21

COMET
Competence Centers for Excellent Technologies

SBA Research

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfw Bundesministerium für Wissenschaft, Forschung und Wirtschaft
FFG
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds