Biases in the RC4 keystream
(128 bit uniform vs. WPA/TKIP)

Nadhem AlFardan and Dan Bernstein and Kenny Paterson and Bertram Poettering and Jacob Schuldt

Royal Holloway, University of London
University of Illinois at Chicago

http://www.isg.rhul.ac.uk/tls/
Keystream distributions at position 1

![Graph showing keystream distributions]

Probability

Byte value [0...255]

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP
Keystream distributions at position 3

![Graph showing keystream distributions at position 3](image-url)
Keystream distributions at position 4

![Graph showing keystream distributions at position 4 with byte values ranging from 0 to 255 and probability values ranging from 0.003878 to 0.00395.](image-url)
Keystream distributions at position 5

Probability vs. Byte value [0...255]
Keystream distributions at position 6

![Graph showing keystream distributions at position 6]

Probability

Byte value [0...255]
Keystream distributions at position 7
Keystream distributions at position 8
Keystream distributions at position 9

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP  9 / 256
Keystream distributions at position 10
Keystream distributions at position 11

![Graph showing keystream distributions at position 11](image)
Keystream distributions at position 12

![Graph showing keystream distributions at position 12]

Probability

Byte value [0...255]
Keystream distributions at position 13
Keystream distributions at position 14

AlFardan et al. (RHUL & UIC)
Keystream distributions at position 15

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP
Keystream distributions at position 16
Keystream distributions at position 17
Keystream distributions at position 18

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 19

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP

19 / 256
Keystream distributions at position 20
Keystream distributions at position 21

![Graph showing keystream distributions at position 21]

Byte value [0...255]
Keystream distributions at position 22

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP   22 / 256
Keystream distributions at position 23

Probability

Byte value [0...255]
Keystream distributions at position 24

Probability

Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP 24 / 256
Keystream distributions at position 25

![Graph showing keystream distributions at position 25. The x-axis represents byte values [0...255] and the y-axis represents probability. The graph shows a red line with a trend that starts from a probability of 0.003878 and increases gradually. There are some sharp peaks at byte values 0 and 16.](image-url)
Keystream distributions at position 26

![Graph showing keystream distributions at position 26. The x-axis represents byte values [0..255], and the y-axis represents probability. There are several spikes at specific byte values.](image-url)
Keystream distributions at position 27
Keystream distributions at position 28

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 29
Keystream distributions at position 30

Probability
Byte value [0...255]

0.003878
0.00390625
0.00395
0  16  32  48  64  80  96  112  128  144  160  176  192  208  224  240  255

Probability
Byte value [0...255]
Keystream distributions at position 31
Keystream distributions at position 32

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 33

![Graph showing keystream distributions at position 33.](image)
Keystream distributions at position 34

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP 34 / 256
Keystream distributions at position 35

![Graph showing keystream distributions at position 35](image-url)
Keystream distributions at position 36

![Graph showing keystream distributions with byte values from 0 to 255 and probability values from 0.00378 to 0.00395.](image_url)
Keystream distributions at position 37

![Graph showing keystream distributions at position 37]
Keystream distributions at position 38

AlFardan et al. (RHUL & UIC) | Biases in RC4 and WPA/TKIP
Keystream distributions at position 39

Probability vs. Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 41

![Graph showing keystream distributions at position 41.](image-url)

- Probability
- Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP

41 / 256
Keystream distributions at position 42

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 43

![Graph showing keystream distributions](image)

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 44

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP 44 / 256
Keystream distributions at position 45

![Graph showing byte value distribution](image)

- Probability distribution for byte values 0 to 255.
- Bias analysis by AlFardan et al. (RHUL & UIC) on biases in RC4 and WPA/TKIP.
Keystream distributions at position 47

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP 47 / 256
Keystream distributions at position 48

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 49

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP

49 / 256
Keystream distributions at position 53

![Graph showing keystream distributions at position 53](image_url)
Keystream distributions at position 54

The graph shows the probability distribution of byte values from 0 to 255. The x-axis represents the byte value, ranging from 0 to 255, and the y-axis represents the probability, which is a range from 0.003878 to 0.00395. There are notable peaks at certain byte values, indicating deviations from a uniform distribution.
Keystream distributions at position 55
Keystream distributions at position 56
Keystream distributions at position 57

![Graph showing keystream distributions at position 57](image-url)
Keystream distributions at position 59

![Graph showing probability distribution of byte values from 0 to 255 at position 59. The graph displays a red line with peaks at specific byte values and a smooth increase across the range.]
Keystream distributions at position 61

![Graph showing keystream distributions at position 61]
Keystream distributions at position 62

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 63
Keystream distributions at position 64

![Graph showing keystream distributions at position 64](image-url)
Keystream distributions at position 65
Keystream distributions at position 66

The graph shows the probability distribution of keystream values at position 66. The x-axis represents byte values [0...255], and the y-axis represents probability. There are peaks around specific byte values, indicating biases in the keystream distribution.
Keystream distributions at position 67
Keystream distributions at position 69

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 70

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP
Keystream distributions at position 71
Keystream distributions at position 72

Probability

Byte value [0...255]

0  16  32  48  64  80  96  112  128  144  160  176  192  208  224  240  255

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 73
Keystream distributions at position 74
Keystream distributions at position 75

Probability

Byte value [0...255]

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP
Keystream distributions at position 76

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP 76 / 256
Keystream distributions at position 77
Keystream distributions at position 79
Keystream distributions at position 81

Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 82

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 83

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP  83 / 256
Keystream distributions at position 84
Keystream distributions at position 85

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP 85 / 256
Keystream distributions at position 87

AlFardan et al. (RHUL & UIC)
Keystream distributions at position 88

![Graph showing the keystream distributions at position 88. The graph plots byte values [0..255] on the x-axis and probability on the y-axis. There are spikes at byte values 96 and 192, indicating higher probabilities at these points.](image-url)
Keystream distributions at position 89
Keystream distributions at position 90

![Graph showing keystream distributions at position 90. The x-axis represents byte values from 0 to 255, and the y-axis represents probability. The graph shows a linear trend with slight fluctuations.](image-url)
Keystream distributions at position 91
Keystream distributions at position 92

Byte value [0...255]

Probability
Keystream distributions at position 93

Probability

Byte value [0...255]
Keystream distributions at position 94

![Graph showing keystream distributions at position 94. The graph plots probability against byte value [0...255]. The x-axis represents byte values from 0 to 255, and the y-axis represents probability values from 0.00378 to 0.0040625. There are peaks at byte values 96 and 112, indicating higher probability at these positions.](image-url)
Keystream distributions at position 95
Keystream distributions at position 96

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 97

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 98

Probability vs. Byte value [0...255]

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 99
Keystream distributions at position 100

![Graph showing keystream distributions at position 100 with probability values for byte values from 0 to 255.](image)

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP

100 / 256
Keystream distributions at position 101
Keystream distributions at position 102

Probability

Byte value [0...255]

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 103
Keystream distributions at position 104

![Graph showing keystream distributions at position 104]

- Probability
- Byte value [0...255]

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 105

![Graph showing keystream distributions at position 105](image)
Keystream distributions at position 106
Keystream distributions at position 107
Keystream distributions at position 108

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 109

![Graph showing keystream distributions at position 109. The graph plots probability against byte value, with a peak at byte value 112.](image)

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 110
Keystream distributions at position 111

![Graph showing keystream distributions at position 111. The x-axis represents byte values [0...255], and the y-axis represents probability. There are two peaks at byte values 112 and 113, indicating higher probabilities compared to other values.]
Keystream distributions at position 112

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 113

![Graph showing byte value distribution from 0 to 255 with probabilities at specific points]

- Probability
- Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP

113 / 256
Keystream distributions at position 114
Keystream distributions at position 115

![Graph showing byte value distribution with probability values at specific byte values]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 116
Keystream distributions at position 117

![Graph showing keystream distributions at position 117](image)

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP

117 / 256
Keystream distributions at position 118

Probability
Byte value [0...255]
Keystream distributions at position 119

![Graph showing keystream distributions at position 119. The x-axis represents byte values from 0 to 255, and the y-axis represents probability values. The graph shows a linear trend with a slight peak at byte value 112.]
Keystream distributions at position 120

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 121
Keystream distributions at position 122
Keystream distributions at position 123
Keystream distributions at position 124

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP 124 / 256
Keystream distributions at position 125
Keystream distributions at position 127

Byte value [0...255]

Probability
Keystream distributions at position 129

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 130

![Graph showing keystream distributions with byte values from 0 to 255 and probabilities ranging from 0.003878 to 0.00395. The graph displays a smooth distribution with a slight increase towards the higher byte values.](image-url)
Keystream distributions at position 131

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP

0  16  32  48  64  80  96  112  128  144  160  176  192  208  224  240  255
Keystream distributions at position 132

![Graph showing keystream distributions at position 132. The x-axis represents byte values [0...255], and the y-axis represents probability. The graph shows a smooth increase in probability as the byte values increase, with some fluctuations around byte value 128.](image-url)
Keystream distributions at position 133

[Graph showing keystream distributions with byte values from 0 to 255 on the x-axis and probabilities on the y-axis.]
Keystream distributions at position 134
Keystream distributions at position 135

![Graph showing probability distribution for byte values 0 to 255 at position 135.](image)
Keystream distributions at position 136

![Graph showing keystream distributions from 0 to 255 bytes with probability values from 0.003878 to 0.00395. The graph includes a line plot with byte values indicated on the x-axis and probability on the y-axis.]
Keystream distributions at position 137
Keystream distributions at position 138
Keystream distributions at position 139
Keystream distributions at position 140

![Graph showing keystream distributions at position 140]

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 141

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP  141 / 256
Keystream distributions at position 142

![Graph showing keystream distributions at position 142]
Keystream distributions at position 143
Keystream distributions at position 144

![Graph showing keystream distributions at position 144]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP 144 / 256
Keystream distributions at position 145

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP

Probability
Byte value [0...255]
Keystream distributions at position 146

![Graph showing keystream distributions with byte values ranging from 0 to 255 and probability values from 0.003878 to 0.00395.]
Keystream distributions at position 147

Probability

Byte value [0...255]
Keystream distributions at position 148

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP  148 / 256
Keystream distributions at position 149

![Graph showing keystream distributions at position 149](image-url)
Keystream distributions at position 150

![Graph showing keystream distributions at position 150. The x-axis represents byte values from 0 to 255, and the y-axis represents probability. The graph exhibits a linear trend with slight variations.](image-url)
Keystream distributions at position 151

![Graph showing keystream distributions at position 151. The graph plots probability against byte value [0..255] with a small peak at byte value 144.]
Keystream distributions at position 152

![Graph showing keystream distributions at position 152 with byte values and probabilities.](image-url)
Keystream distributions at position 153
Keystream distributions at position 154

![Graph showing keystream distributions at position 154. The x-axis represents byte values [0...255] and the y-axis represents probability. The graph indicates a pattern in the keystream distribution.]

AlFardan et al. (RHUL & UIC)
Keystream distributions at position 155
Keystream distributions at position 156

Average probability: 0.0038929

Byte value [0...255]
Keystream distributions at position 157
Keystream distributions at position 158

![Graph showing keystream distributions at position 158]

- Byte values from 0 to 255 are plotted on the x-axis.
- Probability values are shown on the y-axis.
- The graph displays the distribution of keystream values at position 158.
Keystream distributions at position 159

![Graph showing keystream distributions at position 159. The x-axis represents byte values [0..255], and the y-axis represents probability. The graph shows a slight deviation from uniform distribution at certain byte values, particularly at positions 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, and 255.]
Keystream distributions at position 160
Keystream distributions at position 161
Keystream distributions at position 162
Keystream distributions at position 163

![Graph showing keystream distributions at position 163. The x-axis represents byte values from 0 to 255, and the y-axis represents probability. There is a probability distribution with a peak around byte value 163.]
Keystream distributions at position 164

probability

byte value [0...255]

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP
Keystream distributions at position 165

Probability

Byte value [0...255]

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP
Keystream distributions at position 167

![Graph showing keystream distributions at position 167. The x-axis represents byte values from 0 to 255, and the y-axis represents probability. The graph shows a general linear trend with slight variations.](image-url)
Keystream distributions at position 168

Probability
Byte value [0...255]
Keystream distributions at position 169

![Graph showing keystream distributions at position 169. The x-axis represents byte values [0...255] and the y-axis represents probability. The graph shows a smooth distribution with a small peak at a specific byte value.]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 170

Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 171
Keystream distributions at position 172

![Graph showing keystream distributions at position 172. The x-axis represents byte values from 0 to 255, and the y-axis represents probability. The graph shows a flat line across most byte values, with a small spike at byte value 172.]
Keystream distributions at position 173

Probability

Byte value [0...255]
Keystream distributions at position 174

![Graph showing keystream distributions at position 174]
Keystream distributions at position 175

![Graph showing keystream distributions at position 175. The x-axis represents byte values [0...255], and the y-axis shows probability values. There is a significant drop in probability around byte value 176, indicating a bias.]
Keystream distributions at position 177

Probability

Byte value [0...255]
Keystream distributions at position 178
Keystream distributions at position 179
Keystream distributions at position 180
Keystream distributions at position 181

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP
Keystream distributions at position 182

![Graph showing keystream distributions at position 182. The x-axis represents byte values [0...255], and the y-axis represents probability. The graph indicates a trend suggesting a deviation from uniform distribution.]
Keystream distributions at position 184

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 185

![Graph showing keystream distributions at position 185. The x-axis represents byte values [0..255], and the y-axis represents probability. The graph shows a nearly uniform distribution with some slight variations.]

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP
Keystream distributions at position 186
Keystream distributions at position 187
Keystream distributions at position 188

Probability distribution for byte values 0 to 255 at position 188.
Keystream distributions at position 189

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 190
Keystream distributions at position 191

Probability distribution for byte values from 0 to 255 at position 191.

- Probability values range from 0.003878 to 0.00395.
- Byte values shown: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, 255.

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 193
Keystream distributions at position 194
Keystream distributions at position 195

![Graph showing byte value distribution](image-url)
Keystream distributions at position 196
Keystream distributions at position 197

![Graph showing keystream distributions at position 197. The x-axis represents byte values from 0 to 255, and the y-axis represents probability. The graph shows that byte values around 192 have a slightly higher probability compared to others.](image-url)
Keystream distributions at position 198
Keystream distributions at position 199

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC)
Keystream distributions at position 200

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 201

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 202

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
202 / 256
Keystream distributions at position 203

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP  203 / 256
Keystream distributions at position 204
Keystream distributions at position 205

![Graph showing keystream distributions at position 205]

Probability

Byte value [0...255]

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP

205 / 256
Keystream distributions at position 206

0.003878
0.00390625
0.00395

Byte value [0...255]

Probability

0.00390625
0.00390625

Byte value [0...255]

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP
Keystream distributions at position 207
Keystream distributions at position 208

```
<table>
<thead>
<tr>
<th>Byte value [0...255]</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.003878</td>
<td></td>
</tr>
<tr>
<td>0.00390625</td>
<td></td>
</tr>
<tr>
<td>0.00395</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td></td>
</tr>
<tr>
<td>144</td>
<td></td>
</tr>
<tr>
<td>160</td>
<td></td>
</tr>
<tr>
<td>176</td>
<td></td>
</tr>
<tr>
<td>192</td>
<td></td>
</tr>
<tr>
<td>208</td>
<td></td>
</tr>
<tr>
<td>224</td>
<td></td>
</tr>
<tr>
<td>240</td>
<td></td>
</tr>
<tr>
<td>255</td>
<td></td>
</tr>
</tbody>
</table>
```

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP

208 / 256
Keystream distributions at position 209

![Graph showing keystream distributions with byte values and probabilities]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 210

Byte value [0...255] vs. Probability

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP 210 / 256
Keystream distributions at position 211

probability distribution of byte values [0...255]
Keystream distributions at position 212
Keystream distributions at position 213

![Graph showing byte value distribution at position 213 with probabilities 0.003878, 0.00390625, 0.00395, and 0.003878. The x-axis represents byte values from 0 to 255, and the y-axis represents the probability. The graph indicates a general uniform distribution with some variability.]
Keystream distributions at position 214

![Graph showing keystream distributions at position 214. The x-axis represents byte values [0...255], and the y-axis represents probability. The graph shows a nearly flat distribution with slight variations, indicating a uniform distribution of keystream values.](image_url)
Keystream distributions at position 215
Keystream distributions at position 217

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 218

![Graph showing keystream distributions](image-url)

Probability

Byte value [0...255]

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP
Keystream distributions at position 219

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 220
Keystream distributions at position 221

Probability
Byte value [0...255]
Keystream distributions at position 222
Keystream distributions at position 223

Probability

Byte value [0...255]

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP
Keystream distributions at position 224

The graph shows the keystream distributions for byte values ranging from 0 to 255. The x-axis represents the byte value, while the y-axis represents the probability. The graph indicates a relatively even distribution with slight variations at specific points.
Keystream distributions at position 225
Keystream distributions at position 226
Keystream distributions at position 227

![Graph showing keystream distributions at position 227]

- Probability
- Byte value [0...255]
- AlFardan et al. (RHUL & UIC)
- Biases in RC4 and WPA/TKIP
Keystream distributions at position 228
Keystream distributions at position 229

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP

Probability vs. Byte value [0...255]
Keystream distributions at position 230

Probability vs. Byte value [0...255]
Keystream distributions at position 231

![Graph showing the keystream distributions at position 231. The x-axis represents byte values from 0 to 255, and the y-axis represents the probability. The graph indicates a flat distribution with probability values close to 0.00395 for most byte values.](image-url)
Keystream distributions at position 232
Keystream distributions at position 233

Probability
Byte value [0...255]
Keystream distributions at position 234

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP
Keystream distributions at position 235
Keystream distributions at position 236

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP
Keystream distributions at position 238

AlFardan et al. (RHUL & UIC)  Biases in RC4 and WPA/TKIP
Keystream distributions at position 239

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP

239 / 256
Keystream distributions at position 240

Probability
Byte value [0...255]

0.003878
0.00390625
0.00395
0  16  32  48  64  80  96  112  128  144  160  176  192  208  224  240  255

AlFardan et al. (RHUL & UIC) Biases in RC4 and WPA/TKIP

240 / 256
Keystream distributions at position 241
Keystream distributions at position 242

Probability
Byte value [0...255]
Keystream distributions at position 243

Byte value [0...255]

Probability

0  16  32  48  64  80  96  112  128  144  160  176  192  208  224  240  255

Probability

0.00395

0.00390625

0.003878

0.003878
Keystream distributions at position 244

![Graph showing keystream distributions at position 244. The x-axis represents byte values from 0 to 255, and the y-axis represents probability. The graph is a line chart with a slight upward trend towards the end.]
Keystream distributions at position 245

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP
Keystream distributions at position 246

![Graph showing keystream distributions at position 246]
Keystream distributions at position 247

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC)

Biases in RC4 and WPA/TKIP
Keystream distributions at position 248
Keystream distributions at position 249

Byte value [0...255]

Probability

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 250
Keystream distributions at position 251

Probability
Byte value [0...255]
Keystream distributions at position 252

![Graph showing the distribution of keystream values at position 252. The x-axis represents byte values from 0 to 255, and the y-axis represents probability. The graph shows a flat distribution with small variations.]
Keystream distributions at position 253
Keystream distributions at position 254

Probability
Byte value [0...255]

AlFardan et al. (RHUL & UIC)
Biases in RC4 and WPA/TKIP
Keystream distributions at position 255
Keystream distributions at position 256

Probability
Byte value [0...255]