Supplementary Materials

The following table is the mapping table of plaintext, the HM weight of SBOX output value and key calculated by the method in this paper.

# Mapping table of plaintext, the HM weight of SBOX output value and key

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| First round | Second round | Third round | Fourth round | Result |
| Key subset | Selected plaintext | **HM weight** | Key subset | Selected plaintext | **HM weight** | Key subset | Selected plaintext | **HM weight** | Key subset | Selected plaintext | **HM weight** | The Key |
| 0 | **0** | **0** | 251 |  | 251 |
| 1 | **1** | 56 | **83** | **2** | 215 |  | 215 |
| 2 | 78 | **3** | 56 | **1** | **4** | 56 |  | 56 |
| 3 | 115 | 203 | **6** | 203 |  | 203 |
| 4 | 146 | **4** | 115 | **1** | **4** | 158 |  | 158 |
| 5 | 158 | 158 | **5** | 115 |  | 115 |
| 6 | 203 | **5** | 78 |  | 78 |
| 7 | 215 | **6** | 146 |  | 146 |
| 8 | 243 | **7** | 243 |  | 243 |
| 9 | **2** | 6 | **237** | **0** | 22 |  | 22 |
| 10 | 11 | **1** | 163 | **2** | **1** | 213 |  | 213 |
| 11 | 22 | 213 | **5** | 163 |  | 163 |
| 12 | 27 | **2** | 11 | **1** | **3** | 11 |  | 11 |
| 13 | 37 | 230 | **5** | 230 |  | 230 |
| 14 | 54 | **3** | 95 | **5** | **1** | 206 |  | 206 |
| 15 | 61 | 135 | **3** | 135 |  | 135 |
| 16 | 64 | 180 | **4** | 95 |  | 95 |
| 17 | 68 | 206 | **5** | 180 |  | 180 |
| 18 | 95 | **4** | 27 | **12** | **2** | 234 |  | 234 |
| 19 | 101 | 64 | **3** | 64 |  | 64 |
| 20 | 110 | 182 | **5** | 222 |  | 222 |
| 21 | 129 | 222 | **7** | 182 |  | 182 |
| 22 | 132 | 234 | **8** | 27 |  | 27 |
| 23 | 135 | **5** | 6 | **121** | **2** | 68 |  | 68 |
| 24 | 163 | 54 | **3** | 165 |  | 165 |
| 25 | 165 | 68 | **4** | 54 | **1** | **3** | 101 |
| 26 | 180 | 101 | 101 | **4** | 54 |
| 27 | 182 | 110 | **5** | 204 |  | 204 |
| 28 | 195 | 165 | **6** | 6 |  | 6 |
| 29 | 204 | 195 | **7** | 195 |  | 195 |
| 30 | 206 | 204 | **8** | 110 |  | 110 |
| 31 | 213 | **6** | 37 | **3** | **2** | 132 |  | 132 |
| 32 | 222 | 129 | **3** | 129 |  | 129 |
| 33 | 230 | 132 | **5** | 37 |  | 37 |
| 34 | 233 | **7** | 61 | **1** | **3** | 233 |  | 233 |
| 35 | 234 | 233 | **4** | 61 |  | 61 |
| 36 | 250 | **8** | 250 |  | 250 |
| 37 | **3** | 5 | **37** | **1** | 107 | **1** | **1** | 242 |  | 242 |
| 38 | 9 | 242 | **3** | 107 |  | 107 |
| 39 | 10 | **2** | 24 | **177** | **1** | 35 |  | 35 |
| 40 | 14 | 35 | **2** | 223 |  | 223 |
| 41 | 24 | 97 | **3** | 128 | **1** | **2** | 128 |
| 42 | 35 | 128 | 240 | **5** | 240 |
| 43 | 47 | 164 | **4** | 164 |  | 164 |
| 44 | 48 | 207 | **5** | 24 |  | 24 |
| 45 | 49 | 223 | **6** | 207 |  | 207 |
| 46 | 50 | 240 | **7** | 97 |  | 97 |
| 47 | 65 | **3** | 10 | **140** | **1** | 255 |  | 255 |
| 48 | 66 | 47 | **2** | 47 | **1** | **3** | 66 |
| 49 | 67 | 65 | 66 | **5** | 47 |
| 50 | 69 | 66 | **3** | 100 | **1** | **2** | 100 |
| 51 | 73 | 100 | 209 | **7** | 209 |
| 52 | 76 | 103 | **4** | 10 | **2** | **3** | 65 |
| 53 | 87 | 209 | 65 | **6** | 10 |
| 54 | 89 | 218 | **5** | 103 | **1** | **4** | 103 |
| 55 | 92 | 244 | 244 | **5** | 244 |
| 56 | 93 | 255 | **6** | 218 |  | 218 |
| 57 | 97 | **4** | 5 | **18** | **2** | 149 | **1** | **2** | 232 |
| 58 | 100 | 48 | 220 | **4** | 149 |
| 59 | 103 | 67 | 232 | **5** | 220 |
| 60 | 104 | 106 | **3** | 117 |  | 117 |
| 61 | 106 | 117 | **4** | 48 | **1** | **3** | 48 |
| 62 | 107 | 130 | 236 | **4** | 236 |
| 63 | 117 | 149 | **5** | 106 | **3** | **1** | 157 |
| 64 | 128 | 157 | 157 | **5** | 190 |
| 65 | 130 | 178 | 190 | **6** | 106 |
| 66 | 133 | 190 | **6** | 67 | **1** | **3** | 67 |
| 67 | 137 | 220 | 130 | **5** | 130 |
| 68 | 139 | 232 | **7** | 178 |  | 178 |
| 69 | 141 | 236 | **8** | 5 |  | 5 |
| 70 | 142 | **5** | 87 | **46** | **1** | 93 |  | 93 |
| 71 | 149 | 89 | **2** | 141 | **1** | **4** | 152 |
| 72 | 152 | 92 | 152 | **5** | 141 |
| 73 | 157 | 93 | **3** | 194 |  | 194 |
| 74 | 164 | 104 | **4** | 104 | **1** | **5** | 137 |
| 75 | 178 | 137 | 137 | **6** | 104 |
| 76 | 179 | 141 | **5** | 87 | **1** | **3** | 92 |
| 77 | 190 | 142 | 92 | **6** | 87 |
| 78 | 191 | 152 | **6** | 89 |  | 89 |
| 79 | 194 | 194 | **7** | 142 |  | 142 |
| 80 | 196 | **6** | 9 | **168** | **2** | 179 |  | 179 |
| 81 | 207 | 49 | **3** | 139 |  | 139 |
| 82 | 209 | 73 | **4** | 49 | **1** | **3** | 49 |
| 83 | 218 | 76 | 76 | **5** | 76 |
| 84 | 220 | 139 | **5** | 9 |  | 9 |
| 85 | 223 | 179 | **6** | 239 |  | 239 |
| 86 | 232 | 191 | **7** | 73 |  | 73 |
| 87 | 236 | 239 | **8** | 191 |  | 191 |
| 88 | 239 | **7** | 14 | **10** | **2** | 196 |  | 196 |
| 89 | 240 | 69 | **4** | 69 |  | 69 |
| 90 | 242 | 133 | **5** | 133 |  | 133 |
| 91 | 244 | 196 | **7** | 14 |  | 14 |
| 92 | 255 | **8** | 50 |  | 50 |
| 93 | **4** | 0 | **167** | **1** | 53 | **3** | **1** | 212 |  | 212 |
| 94 | 2 | 57 | **2** | 53 |  | 53 |
| 95 | 3 | 159 | **4** | 159 |  | 159 |
| 96 | 7 | 212 | **5** | 57 |  | 57 |
| 97 | 13 | **2** | 2 | **98** | **1** | 17 | **1** | **4** | 17 |
| 98 | 16 | 17 | 145 | **6** | 145 |
| 99 | 17 | 19 | **2** | 188 | **2** | **3** | 188 |
| 100 | 18 | 32 | 227 | **7** | 227 |
| 101 | 19 | 145 | **3** | 32 |  | 32 |
| 102 | 21 | 188 | **4** | 19 |  | 19 |
| 103 | 28 | 201 | **5** | 201 |  | 201 |
| 104 | 32 | 227 | **6** | 248 |  | 248 |
| 105 | 34 | 248 | **7** | 2 |  | 2 |
| 106 | 36 | **3** | 3 | **2** | **2** | 39 | **3** | **4** | 39 |
| 107 | 39 | 21 | 228 | **5** | 228 |
| 108 | 41 | 34 | **3** | 151 | **1** | **2** | 205 |
| 109 | 51 | 39 | 205 | **3** | 238 |
| 110 | 52 | 41 | 238 | **6** | 151 |
| 111 | 53 | 79 | **4** | 34 | **3** | **4** | 88 |
| 112 | 55 | 83 | 88 | **5** | 34 |
| 113 | 57 | 88 | **5** | 3 | **3** | **3** | 79 |
| 114 | 60 | 123 | 79 | **4** | 3 |
| 115 | 70 | 125 | 123 | **5** | 123 |
| 116 | 79 | 151 | 173 | **6** | 173 |
| 117 | 80 | 162 | **6** | 83 | **1** | **4** | 83 |
| 118 | 82 | 173 | 125 | **5** | 125 |
| 119 | 83 | 205 | **7** | 41 | **1** | **2** | 162 |
| 120 | 88 | 228 | 162 | **3** | 254 |
| 121 | 90 | 238 | 254 | **5** | 41 |
| 122 | 91 | 254 | **8** | 21 |  | 21 |
| 123 | 98 | **4** | 0 | **68** | **1** | 183 |  | 183 |
| 124 | 102 | 13 | **2** | 0 | **1** | **3** | 197 |
| 125 | 109 | 16 | 197 | **5** | 0 |
| 126 | 113 | 51 | **3** | 13 | **1** | **5** | 13 |
| 127 | 123 | 60 | 155 | **6** | 155 |
| 128 | 125 | 98 | **4** | 167 | **1** | **4** | 167 |
| 129 | 134 | 148 | 170 | **5** | 170 |
| 130 | 138 | 155 | **5** | 16 | **1** | **2** | 60 |
| 131 | 145 | 167 | 60 | **4** | 16 |
| 132 | 148 | 170 | 98 | **5** | 98 |
| 133 | 151 | 183 | **6** | 51 |  | 51 |
| 134 | 153 | 197 | **7** | 148 |  | 148 |
| 135 | 155 | **5** | 18 | **58** | **1** | 237 |  | 237 |
| 136 | 156 | 28 | **2** | 211 | **1** | **4** | 249 |
| 137 | 159 | 36 | 249 | **5** | 211 |
| 138 | 162 | 52 | **3** | 52 | **4** | **3** | 52 |
| 139 | 166 | 80 | 80 | **5** | 80 |
| 140 | 167 | 82 | 82 | **6** | 82 |
| 141 | 170 | 90 | **4** | 134 | **1** | **2** | 134 |
| 142 | 173 | 134 | 166 | **4** | 166 |
| 143 | 176 | 166 | **5** | 18 | **1** | **4** | 18 |
| 144 | 183 | 211 | 28 | **5** | 28 |
| 145 | 184 | 237 | **6** | 36 |  | 36 |
| 146 | 185 | 249 | **7** | 90 |  | 90 |
| 147 | 188 | **6** | 55 | **35** | **1** | 109 |  | 109 |
| 148 | 197 | 102 | **2** | 217 | **2** | **3** | 246 |
| 149 | 199 | 109 | 246 | **5** | 217 |
| 150 | 201 | 113 | **3** | 102 | **2** | **1** | 156 |
| 151 | 205 | 138 | 156 | **3** | 102 |
| 152 | 211 | 153 | **4** | 113 | **1** | **4** | 184 |
| 153 | 212 | 156 | 184 | **5** | 113 |
| 154 | 217 | 184 | **5** | 138 |  | 138 |
| 155 | 227 | 185 | **6** | 55 | **1** | **2** | 55 |
| 156 | 228 | 217 | 185 | **4** | 185 |
| 157 | 237 | 246 | **7** | 153 |  | 153 |
| 158 | 238 | **7** | 7 | **6** | **2** | 70 |  | 70 |
| 159 | 246 | 70 | **3** | 91 |  | 91 |
| 160 | 248 | 91 | **5** | 7 |  | 7 |
| 161 | 249 | 199 | **6** | 199 |  | 199 |
| 162 | 254 | **8** | 176 |  | 176 |
| 163 | **5** | 1 | **111** | **1** | 33 | **1** | **3** | 241 |  | 241 |
| 164 | 12 | 241 | **4** | 33 |  | 33 |
| 165 | 15 | 253 | **7** | 253 |  | 253 |
| 166 | 26 | **2** | 1 | **10** | **1** | 121 |  | 121 |
| 167 | 29 | 74 | **2** | 1 | **1** | **4** | 1 |
| 168 | 33 | 116 | 74 | **5** | 74 |
| 169 | 38 | 121 | **3** | 219 |  | 219 |
| 170 | 40 | 161 | **4** | 172 |  | 172 |
| 171 | 42 | 172 | **5** | 161 | **1** | **4** | 177 |
| 172 | 46 | 177 | 177 | **7** | 161 |
| 173 | 58 | 219 | **6** | 116 |  | 116 |
| 174 | 63 | 235 | **7** | 235 |  | 235 |
| 175 | 72 | **3** | 26 | **57** | **1** | 171 |  | 171 |
| 176 | 74 | 38 | **2** | 247 |  | 247 |
| 177 | 75 | 42 | **3** | 26 | **3** | **3** | 94 |
| 178 | 77 | 46 | 94 | **6** | 26 |
| 179 | 84 | 94 | **4** | 42 | **1** | **3** | 221 |
| 180 | 94 | 131 | 221 | **7** | 42 |
| 181 | 99 | 171 | **5** | 181 | **1** | **2** | 181 |
| 182 | 111 | 181 | 226 | **4** | 226 |
| 183 | 112 | 221 | **6** | 38 |  | 38 |
| 184 | 114 | 226 | **7** | 131 |  | 131 |
| 185 | 116 | 247 | **8** | 46 |  | 46 |
| 186 | 118 | **4** | 63 | **18** | **1** | 140 |  | 140 |
| 187 | 120 | 72 | **2** | 77 | **1** | **3** | 77 |
| 188 | 121 | 75 | 124 | **4** | 124 |
| 189 | 122 | 77 | **3** | 75 | **1** | **4** | 122 |
| 190 | 124 | 111 | 122 | **5** | 75 |
| 191 | 131 | 122 | **4** | 72 | **1** | **2** | 111 |
| 192 | 136 | 124 | 111 | **3** | 72 |
| 193 | 140 | 140 | **5** | 187 | **1** | **4** | 229 |
| 194 | 143 | 168 | 229 | **7** | 187 |
| 195 | 147 | 187 | **6** | 63 | **1** | **4** | 216 |
| 196 | 161 | 216 | 216 | **6** | 63 |
| 197 | 168 | 229 | **7** | 168 |  | 168 |
| 198 | 169 | **5** | 12 | **142** | **1** | 192 |  | 192 |
| 199 | 171 | 29 | **2** | 136 |  | 136 |
| 200 | 172 | 99 | **3** | 12 | **2** | **3** | 12 |
| 201 | 175 | 114 | 210 | **7** | 210 |
| 202 | 177 | 136 | **4** | 99 | **3** | **3** | 189 |
| 203 | 181 | 175 | 189 | **7** | 99 |
| 204 | 187 | 189 | **5** | 29 | **1** | **4** | 29 |
| 205 | 189 | 192 | 175 | **6** | 175 |
| 206 | 192 | 210 | **6** | 231 |  | 231 |
| 207 | 210 | 231 | **7** | 114 |  | 114 |
| 208 | 216 | **6** | 40 | **116** | **0** | 143 |  | 143 |
| 209 | 219 | 58 | **1** | 58 |  | 58 |
| 210 | 221 | 84 | **2** | 245 |  | 245 |
| 211 | 226 | 112 | **3** | 40 |  | 40 |
| 212 | 229 | 118 | **4** | 84 | **2** | **5** | 118 |
| 213 | 231 | 143 | 118 | **6** | 84 |
| 214 | 235 | 169 | **5** | 169 |  | 169 |
| 215 | 241 | 245 | **7** | 112 |  | 112 |
| 216 | 245 | **7** | 15 | **1** | **1** | 147 |  | 147 |
| 217 | 247 | 147 | **3** | 15 |  | 15 |
| 218 | 253 | **8** | 120 |  | 120 |
| 219 | **6** | 8 | **168** | **1** | 127 | **1** | **4** | 144 |  | 144 |
| 220 | 20 | 144 | **6** | 127 |  | 127 |
| 221 | 25 | **2** | 30 | **9** | **2** | 44 |  | 44 |
| 222 | 30 | 44 | **3** | 198 |  | 198 |
| 223 | 31 | 174 | **4** | 174 |  | 174 |
| 224 | 44 | 198 | **8** | 30 |  | 30 |
| 225 | 45 | **3** | 45 | **8** | **1** | 154 |  | 154 |
| 226 | 59 | 71 | **2** | 45 |  | 45 |
| 227 | 62 | 108 | **3** | 108 |  | 108 |
| 228 | 71 | 119 | **4** | 71 |  | 71 |
| 229 | 81 | 154 | **6** | 119 |  | 119 |
| 230 | 85 | **4** | 20 | **49** | **0** | 202 |  | 202 |
| 231 | 86 | 31 | **2** | 20 |  | 20 |
| 232 | 105 | 81 | **3** | 86 |  | 86 |
| 233 | 108 | 86 | **5** | 31 |  | 31 |
| 234 | 119 | 202 | **7** | 81 |  | 81 |
| 235 | 126 | **5** | 25 | **2** | **2** | 25 |  | 25 |
| 236 | 127 | 59 | **3** | 85 |  | 85 |
| 237 | 144 | 85 | **4** | 59 |  | 59 |
| 238 | 150 | 224 | **5** | 224 |  | 224 |
| 239 | 154 | **6** | 62 | **32** | **2** | 150 |  | 150 |
| 240 | 174 | 105 | **3** | 105 |  | 105 |
| 241 | 193 | 126 | **4** | 214 |  | 214 |
| 242 | 198 | 150 | **5** | 126 |  | 126 |
| 243 | 200 | 193 | **6** | 62 |  | 62 |
| 244 | 202 | 214 | **7** | 193 |  | 193 |
| 245 | 214 | **7** | 8 | **1** | **3** | 8 |  | 8 |
| 246 | 224 | 200 | **4** | 200 |  | 200 |
| 247 | **7** | 4 | **7** | **0** | 252 |  | 252 |
| 248 | 43 | **1** | 208 |  | 208 |
| 249 | 96 | **2** | 225 |  | 225 |
| 250 | 160 | **3** | 96 |  | 96 |
| 251 | 186 | **4** | 4 | **1** | **3** | 4 |  | 4 |
| 252 | 208 | 160 | **5** | 160 |  | 160 |
| 253 | 225 | **5** | 186 |  | 186 |
| 254 | 252 | **6** | 43 |  | 43 |
| 255 | **8** | 23 |  | 23 |