

Figure 1: Caption

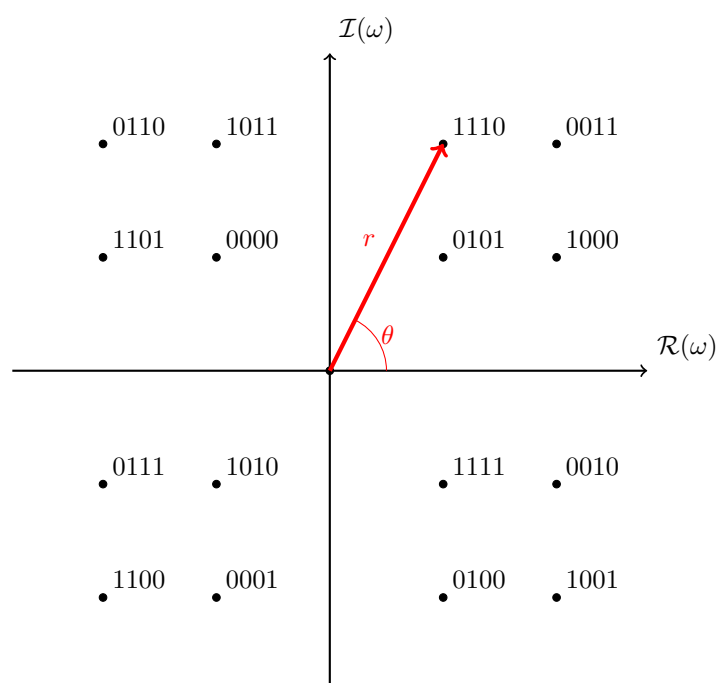
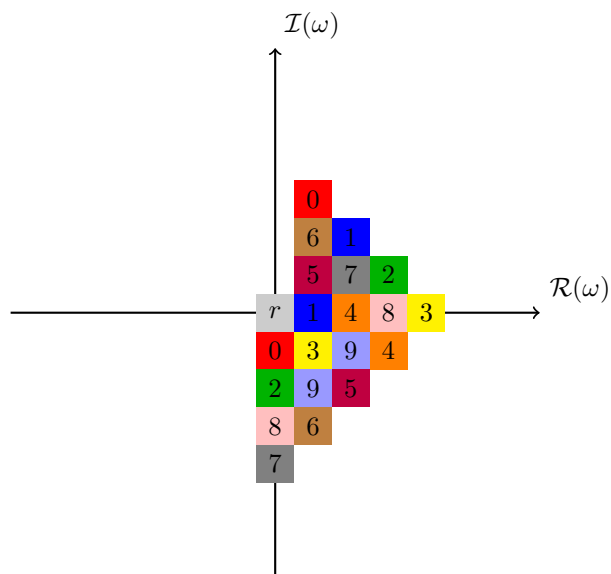


Figure 2: Encoding 4-bit words into frequencies.



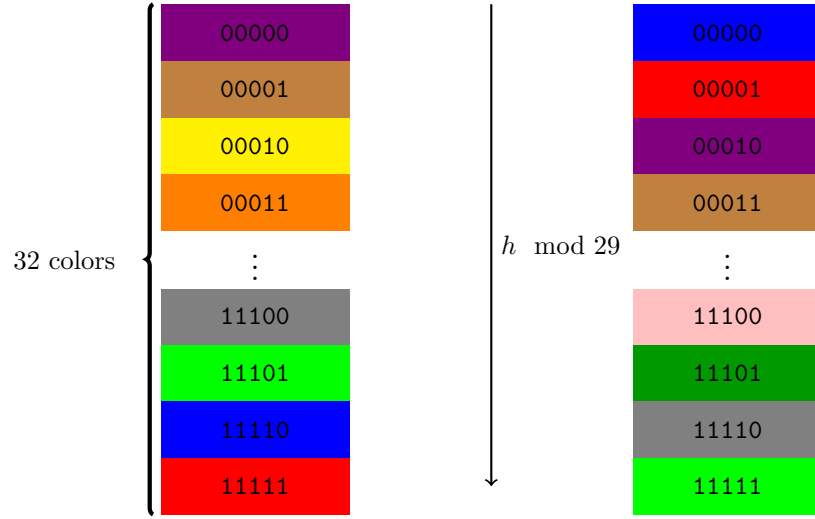
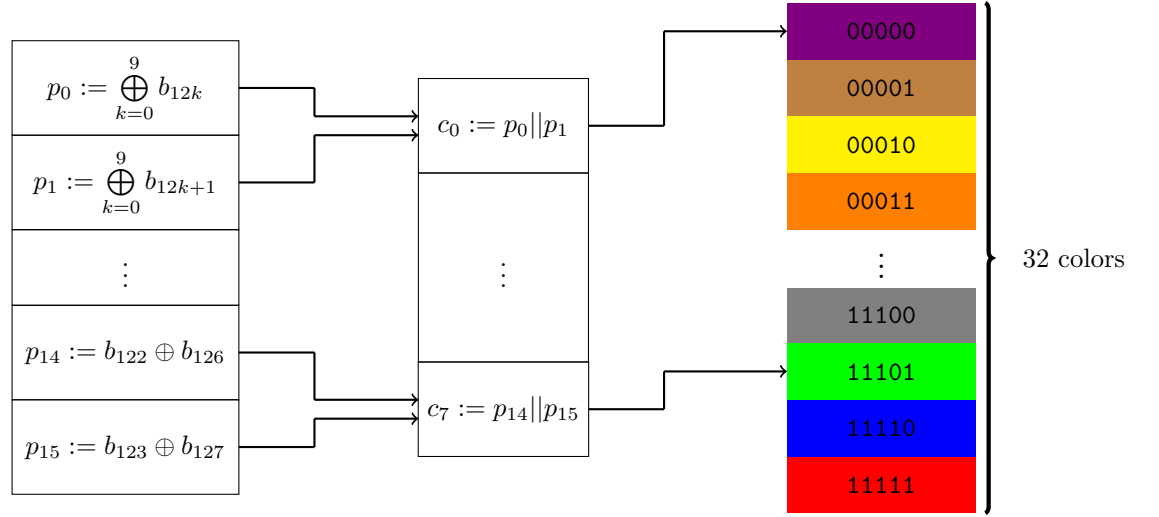
$$\mathcal{B}_m = I(f_m > 0.5), \quad m \in \{1, 2, 3\}$$

$$\mathcal{P}(\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}) \rightarrow \{Color\#1, Color\#2, \dots, Color\#2^m\}$$

$$\begin{aligned} \{Color\#1, Color\#2, \dots, Color\#2^m\} = & \{f_1 \leq 0.5 \wedge f_2 \leq 0.5 \wedge f_3 \leq 0.5, \\ & f_1 \leq 0.5 \wedge f_2 \leq 0.5 \wedge f_3 > 0.5, \\ & \dots, \\ & f_1 > 0.5 \wedge f_2 > 0.5 \wedge f_3 > 0.5 \end{aligned}$$

$$h = \underbrace{\underline{1100}}_{f_1} \underbrace{\underline{1000}}_{f_2} \underbrace{\underline{0110}}_{f_3} \underbrace{\underline{1110}} \underbrace{\underline{0101}} \underbrace{\underline{1011}} \underbrace{\underline{0100}} \underbrace{\underline{1111}} \underbrace{\underline{0110}} \underbrace{\underline{0010}} \underbrace{\underline{1001}} \underbrace{\underline{0110}} \dots \underbrace{\underline{0010}} \underbrace{\underline{1001}} \underbrace{\underline{0101}} \underbrace{\underline{1001}} \underbrace{\underline{0100}}$$

$$p_i = \begin{cases} b_{0,i} \oplus b_{1,i} \oplus b_{2,i} \oplus \cdots \oplus b_{9,i} = \bigoplus_{k=0}^9 b_{k,i} & 0 \leq i < 12 \\ h_{120+i-12} \oplus h_{120+i-8} & 12 \leq i < 16 \end{cases}$$



Proof that $\tilde{x} \neq x \bmod 23$, where \tilde{x} is x with 2 bits of the same group changed: Let ℓ and $\ell + 12m$ the indices of the 2 flipped bits, with $0 < m \leq 10$. Ring of \mathbb{Z}_p is an integral domain.

- Case $b_\ell = 1, b_{\ell+12m} = 0$:

$$\begin{aligned}
x &= \tilde{x} = x - 2^\ell + 2^{\ell+12m} \pmod{23} \\
\implies x &= x + 2^\ell (2^{12m} - 1) \pmod{23} \\
\implies 0 &= 2^\ell (2^{12m} - 1) \pmod{23} \\
\implies 0 &= 2^{12m} - 1 \pmod{23} \\
\implies 1 &= 2^{12m} \pmod{23}
\end{aligned}$$

which has no solution for $1 < m \leq 10$.

- Case $b_\ell = 0, b_{\ell+12m} = 1$:

$$\begin{aligned}
x &= \tilde{x} = x - 2^\ell + 2^{\ell+12m} \pmod{23} \\
\implies x &= x + 2^\ell (1 - 2^{12m}) \pmod{23} \\
\implies 0 &= 2^\ell (1 - 2^{12m}) \pmod{23}
\end{aligned}$$

which has no solution for $1 < m \leq 10$, same as the previous case.

- Case $b_\ell = 1, b_{\ell+12m} = 1$:

$$\begin{aligned}
x &= \tilde{x} = x + 2^\ell + 2^{\ell+12m} \pmod{23} \\
\implies x &= x + 2^\ell (1 + 2^{12m}) \pmod{23} \\
\implies 0 &= 2^\ell (1 + 2^{12m}) \pmod{23} \\
\implies 0 &= 1 + 2^{12m} \pmod{23} \\
\implies -1 &= 2^{12m} \pmod{23}
\end{aligned}$$

which has no solution for $1 < m \leq 10$.

- Case $b_\ell = 0, b_{\ell+12m} = 0$:

$$\begin{aligned}
x &= \tilde{x} = x - 2^\ell - 2^{\ell+12m} \pmod{23} \\
\implies x &= x + 2^\ell (-1 - 2^{12m}) \pmod{23} \\
\implies 0 &= 2^\ell (-1 - 2^{12m}) \pmod{23}
\end{aligned}$$

which has no solution for $1 < m \leq 10$, same as the previous case

Attacks if shift is $\pmod{23}$:

- Adv flips n bits of the same index, keeping same modulo 23 :
 - Effect : the same palette is used. If n is even and $n > 2$, then all colors are exactly the same as intra group parity is the same

- "Impossible" for odd n as palette is flipped
- Rare (I guess) for $n = 4$: maximum 8 if the ten bits are e.g. 1101011100
- Adv flips n bits, keeping same modulo 23 :
 - Effect : the same palette is used. The colors corresponding to the n indices are changed
 - "Impossible" for odd n as palette is flipped

$$\begin{aligned}
 x + 2^k - 2^\ell &= x \pmod{p} \\
 2^k - 2^\ell &= 0 \pmod{p} \\
 2^\ell (2^{k-\ell} - 1) &= 0 \pmod{p} \\
 2^{k-\ell} &= 1 \pmod{p} \\
 k - \ell &= m \cdot |2| \pmod{p}, \quad m \in \mathbb{Z}
 \end{aligned}$$

Problem : 11 is $-1 \pmod{12} \implies$ flipping b_i and b_{i+11} might only change 1 color.

Attacks if shift is $\sum index$:

Lots (sum of 4 indices that are for the same function divide 31)

Properties:

- Color choices : $\{(b_0 \oplus b_{12} \oplus \dots \oplus b_{108}), (b_1 \oplus b_{13} \oplus \dots \oplus b_{109}), \dots, (b_{11} \oplus \dots \oplus b_{119})\}$
- Palette shift : $h \pmod{23}$
- Invert palette direction : $w(h) \pmod{2}$
- Symmetry mode : $\sum_{i:h_i=1} i + 11 \pmod{13}$

Keeping same parity bits :

$$b'_0 \oplus b'_{12} \oplus \dots \oplus b'_{108} = b_0 \oplus b_{12} \oplus \dots \oplus b_{108}$$

$$\bigoplus_{i=0}^9 b'_{12i} = \bigoplus_{i=0}^{10} b_{12i}$$

Implications :

- If $b'_i \neq b_i$ for an odd number of i , then the parity of the weight of h changes and the palette is flipped.
- To keep the same palette shift, we must have $h = h' \pmod{23}$, with $h' = h + \sum_k 2^k - \sum_\ell 2^\ell$ for all $k : b_k = 0 \wedge b'_k = 1$ and $\ell : b_\ell = 1 \wedge b'_\ell = 0$. Because of the previous point, we must have $k + \ell = 0 \pmod{2}$.

$$h + \sum_k 2^k - \sum_\ell 2^\ell = h \pmod{23}$$

$$\sum_k 2^k - \sum_\ell 2^\ell = 0 \pmod{23}$$

$$|2| \pmod{23} = 11 \implies 2^{12i} \pmod{23} = (2^{12})^i \pmod{23} = (2 \cdot 2^{11})^i \pmod{23} = 2^i \pmod{23}.$$

$$2^{12i} \pmod{23} = 2^i \pmod{23} \text{ for } i \in \{0, \dots, 9\} = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6\} := M$$

For $n = 2, 4, 6, 8, 10$: find n distinct elements $m_i \in M$ and a vector $\alpha \in \{-1, 1\}^n$ such that $\sum_{i=0}^9 \alpha_i m_i = 0 \pmod{23}$

- $n = 2$: It is impossible to find $m_1 \neq m_2$ such that $m_1 \pm m_2 = 0 \pmod{23}$.
- $n = 4$: With Python, we found there are 84 possible choices for m_0, m_1, m_2, m_3 such that we can find a fitting α . For example, $m_1 = 2, m_2 = 4, m_3 = 16, m_4 = 18$, we find $\alpha = \{1, -1, -1, 1\}$.
- $n = 6$: We found there are 280 possible choices for m_0 to m_5 such that we can find a fitting α .
- $n = 8$: We found there are 255 possible choices for m_0 to m_7 such that we can find a fitting α .
- $n = 10$: Picking m_0 to m_9 as every element of M , we can find (for example) $\alpha = \{1, -1, -1, 1, -1, 1, -1, 1, 1, 1\}$ that is fitting.
- In total, 620 "collisions" with same parity and same palette shift

Introducing the symmetries: in order to keep the same symmetry, we must have $\sum_{i:h_i=1} i + 11 \pmod{13} = \sum_{i:h'_i=1} i + 11 \pmod{13}$. That means a collision must have $\sum 12m_i \alpha_i = 0 \pmod{13}$

- $n = 4$: The number of collision drops to 53 (IN TOTAL):.
- $n = 6$: We found there are 292 (IN TOTAL) possible collisions.
- $n = 8$: We found there are 230 (IN TOTAL) possible collisions.
- $n = 10$: We found there are 25 (IN TOTAL) possible collisions).
- In total, 620 "collisions" with same parity and same palette shift
- However, each requires a specific combination of bits to be possible. Some of them are mutually exclusive. \rightarrow divide by $\approx 16, 32, 64 \rightarrow$

If the bits are not from the same parity:

If two flipped bits of same value:

Same shift :

$$\begin{aligned} h + 2^k + 2^\ell &= h \pmod{p} \\ 2^k + 2^\ell &= 0 \pmod{p} \\ 2^\ell(2^{k-\ell} + 1) &= 0 \pmod{p} \\ 2^{k-\ell} &= -1 \pmod{p} \end{aligned}$$

Which is not possible as long as we pick $p \neq 3$ and $p \neq 17$

Same shift :

$$\begin{aligned} h + 2^k - 2^\ell &= h \pmod{p} \\ 2^k - 2^\ell &= 0 \pmod{p} \\ 2^\ell(2^{k-\ell} - 1) &= 0 \pmod{p} \\ 2^{k-\ell} &= 1 \pmod{p} \\ k - \ell &= 0 \pmod{(|2| \pmod{p})} \end{aligned}$$

Same symmetry :

$$k - \ell = 0 \pmod{(|2| \pmod{q})}$$

Having both yield

$$k - \ell = 0 \pmod{\text{lcm}(|2| \pmod{p}, |2| \pmod{q})}$$

If we pick $p = 29, q = 23$ we have $(|2| \pmod{p}, |2| \pmod{q}) = (28, 11)$ and $\text{lcm}(28, 11) = 308 > 256$

oui $h = 101011101010101\dots1010011110111$