

One algorithm is the following.

```

For  $i = 1, 2, \dots, n$ 
  Receiver  $j$  computes  $\beta_{ij} = f(\beta_1^* \cdots \beta_{i-1}^*, \alpha_i^{(j)})$ .
   $\beta_i^*$  is set to the majority value of  $\beta_{ij}$ , for  $j = 1, \dots, k$ .
End for
Output  $\beta^*$ 

```

We'll make sure to choose an odd value of k to prevent ties.

Let $X_{ij} = 1$ if $\alpha_i^{(j)}$ was corrupted, and 0 otherwise. If a majority of the bits in $\{\alpha_i^{(j)} : j = 1, 2, \dots, k\}$ are corrupted, then $X_i = \sum_j X_{ij} > k/2$. Now, since each bit is corrupted with probability $\frac{1}{4}$, $\mu = \sum_j EX_{ij} = k/4$. Thus, by the Chernoff bound, we have

$$\begin{aligned}
 \Pr[X_i > k/2] &= \Pr[X_i > 2\mu] \\
 &< \left(\frac{e}{4}\right)^{k/4} \\
 &\leq (.91)^k.
 \end{aligned}$$

Now, if

$$k \geq 11 \ln n > \frac{\ln n - \ln .1}{\ln(1/.91)},$$

then

$$\Pr[X_i > k/2] < .1/n.$$

(So it is enough to choose k to be the smallest odd integer greater than $11 \ln n$.) Thus, by the union bound, the probability that *any* of the sets $\{\alpha_i^{(j)} : j = 1, 2, \dots, k\}$ have a majority of corruptions is at most .1.

Assuming that a majority of the bits in each of these sets are not corrupted, which happens with probability at least .9, one can prove by induction on i that all the bits in the reconstructed message β^* will be correct.

¹ex482.918.336