Virtual Lib

Let $p_{\textsf{fail}}$, a failure probability and $z^*\left(p_{\textsf{fail}}\right)$, the associated standard score i.e.

$$z^*\left(p_{\textsf{fail}}\right) = \sqrt{2} \cdot \textsf{erf}^{-1}(1 - p_{\textsf{fail}})$$

An error happens when we decode the plaintext and instead of getting the right value, we end up with our value plus or minus a small error i.e. $\left\lfloor \frac{\Delta \cdot m + e}{\Delta} \right\rceil = m + \left\lfloor \frac{e}{\Delta} \right\rceil$. The purpose of this document is to find the distribution X of this error.

To satisfy the $p_{\textsf{fail}}$ constraint, the optimizer will find parameters such that with e the noise in the ciphertext coming from a normal distribution $\mathcal{N}(0, \sigma^2)$ and Δ, the scaling factor (where the message starts), we have

$$\mathbb{P}\left(|e| < \frac{\Delta}{2}\right) = 1 - p_{\textsf{fail}} \text{ i.e. } \mathbb{P}\left(\underbrace{\left\lfloor \frac{e}{\Delta} \right\rceil}_{=F} = 0\right) = 1 - p_{\textsf{fail}}$$

by enforcing that $z^*\left(p_{\textsf{fail}}\right) \cdot \sigma \leq \Delta/2$. To simplify the rest of the document, we will assume $z^*\left(p_{\textsf{fail}}\right) \cdot \sigma = \Delta/2$

and so we have

$$\mathbb{P}\left(F = 0\right) = \mathbb{P}\left(|e| < \frac{\Delta}{2}\right) = 1 - p_{\textsf{fail}}$$

Now let's find $\mathbb{P}\left(F = k\right), \forall k$

$$\begin{aligned}
\mathbb{P}\left(F = 1\right) = \mathbb{P}\left(\frac{\Delta}{2} < |e| < \frac{3\,\Delta}{2}\right) \\
&= \mathbb{P}\left(|e| < \frac{3\,\Delta}{2}\right) - \mathbb{P}\left(|e| < \frac{\Delta}{2}\right) \\
&= \mathbb{P}\left(|e| < 3 \cdot z^*\left(p_{\textsf{fail}}\right) \cdot \sigma\right) - \left(1 - p_{\textsf{fail}}\right)
\end{aligned}$$

We can once again use the normal confidence interval to compute the first probability as we have

$$\mathbb{P}\left(|e| < 3 \cdot z^*\left(p_{\mathsf{fail}}\right) \cdot \sigma\right) = \mathsf{erf}\left(\frac{3 \cdot z^*\left(p_{\mathsf{fail}}\right)}{\sqrt{2}}\right)$$

We can keep going for other values

$$\begin{aligned}\mathbb{P}\left(F = 2\right) &= \mathbb{P}\left(\frac{3\,\Delta}{2} < |e| < \frac{5\,\Delta}{2}\right) \\ &= \mathbb{P}\left(|e| < \frac{5\,\Delta}{2}\right) - \mathbb{P}\left(|e| < \frac{3\,\Delta}{2}\right) \\ &= \mathbb{P}\left(|e| < 5 \cdot z^*\left(p_{\mathsf{fail}}\right) \cdot \sigma\right) - \mathbb{P}\left(|e| < 3 \cdot z^*\left(p_{\mathsf{fail}}\right) \cdot \sigma\right)\end{aligned}$$

More generally, we have

$$\begin{aligned}\forall k > 0, \mathbb{P}\left(F = k\right) &= \mathbb{P}\left(\frac{\Delta}{2} + (k-1) \cdot \Delta < |e| < \frac{\Delta}{2} + k \cdot \Delta\right) \\ &= \mathbb{P}\left(|e| < \Delta \cdot (k + \frac{1}{2})\right)) - \mathbb{P}\left(\Delta \cdot (k - \frac{1}{2}) < |e|\right) \\ &= \mathbb{P}\left(|e| < z^*\left(p_{\mathsf{fail}}\right) \cdot (2\,k+1) \cdot \sigma)\right) \\ &- \mathbb{P}\left(z^*\left(p_{\mathsf{fail}}\right) \cdot (2\,k-1) \cdot \sigma < |e|\right)\end{aligned}$$

Using the formula below, we can compute the distribution of the errors:

$$\mathbb{P}\left(|e| < (2k+1) \cdot z^*\left(p_{\mathsf{fail}}\right) \cdot \sigma\right) = \mathsf{erf}\left(\frac{(2k+1) \cdot z^*\left(p_{\mathsf{fail}}\right)}{\sqrt{2}}\right)$$