① 1. $\Pr\left[e_i \le \frac{p}{4\ell} \quad \forall i = 1, \dots, \underset{\#\text{samples}}{\ell}\right] = \Pr\left[e_1 \le \frac{p}{4\ell} \cap \dots \cap e_\ell \le \frac{p}{4\ell}\right]$

$$= \prod_{i=1}^{m} \Pr\left[e_i \le \frac{p}{4\ell}\right] \quad \text{(due to independence of } e_i\text{'s)}$$

$$= \prod_{i=1}^{m} \left(1 - \Pr\left(e_i > \frac{p}{4\ell}\right]\right)$$

$$= \left(1 - \Pr\left[e > \frac{p}{4\ell}\right]\right)^{\ell} \quad \text{(due to randomness of } e_i\text{'s)}$$

$$\ge (1 - B)^{\ell}$$

since $\Pr\Big[e > \underbrace{\frac{p}{4\ell}}_{\text{not an integer since } p \text{ is a prime}}\Big] = \Pr\Big[e \ge \underbrace{\left\lceil \frac{p}{4\ell} \right\rceil}_{\text{must be an integer}}\Big] \le \dfrac{\sigma}{v\left(\left\lceil \frac{p}{4\ell}\right\rceil - 1\right)\sqrt{2\pi}} \cdot e^{-\left(\left\lceil \frac{p}{4\ell}\right\rceil - 1\right)^2 / 2\sigma^2}$

due to fact 1

$$\le \frac{\sigma}{\left(1 - \frac{1}{\sqrt{2\pi}\sigma} \cdot e^{-1}\right)\left(\left\lceil \frac{p}{4\ell}\right\rceil - 1\right)\sqrt{2\pi}} \cdot e^{-\left(\left\lceil \frac{p}{4\ell}\right\rceil - 1\right)^2 / 2\sigma^2} := B$$

2. $m' = \left\lfloor \frac{2}{p}(c_1 - c_0 \cdot s) \right\rceil = \left\lceil \frac{2}{p}\left(m\frac{p-1}{2} + \sum_{i=1}^{\ell} r_i \cdot \underset{\text{size } n}{b_i} - s \cdot \sum_{i=1}^{\ell} r_i \cdot \underset{\text{size } n}{a_i}\right)\right\rfloor$ — a_i: i-th row of A (a sample)

$$= \left\lceil \frac{2}{p}\left(m\frac{p-1}{2} + \sum_{i=1}^{\ell} r_i \cdot (a_i \cdot s + e_i) - s \cdot \sum_{i=1}^{\ell} r_i \cdot a_i\right)\right\rfloor \quad a_i\text{: i-th row of A}$$

$$= \left\lceil \frac{2}{p}\left(m\frac{p-1}{2} + \sum_{i=1}^{\ell} r_i \cdot e_i\right)\right\rfloor$$

$$= \left\lceil m \cdot \frac{p-1}{p} + \frac{2}{p} \sum_{i=1}^{\ell} r_i \cdot e_i \right\rfloor$$

Due to the rounding fct. we can recover m if $\left|\frac{2}{p} \sum_{i=1}^{\ell} r_i \cdot e_i\right| \le \frac{1}{2}$, i.e., $\left|\sum_{i=1}^{\ell} r_i \cdot e_i\right| \le \frac{p}{4}$.

Otherwise decryption fails and its probability is computed as follows:

$\Pr[\text{decryption failure}] = \Pr\left[\left|\sum_{i=1}^{\ell} r_i \cdot e_i\right| > \frac{p}{4}\right] = 1 - \Pr\left[\left|\sum_{i=1}^{\ell} r_i \cdot e_i\right| \le \frac{p}{4}\right]$ and observe that

$$\Pr\left[\left|\sum_{i=1}^{\ell} r_i \cdot e_i\right| \le \frac{p}{4}\right] \ge \Pr\left[\sum_{i=1}^{\ell} |r_i \cdot e_i| \le \frac{p}{4}\right] \ge \Pr\left[\sum_{i=1}^{\ell} |e_i| \le \frac{p}{4}\right] = \Pr\left[\ell \cdot e \le \frac{p}{4}\right] = \Pr\left[e \le \frac{p}{4\ell}\right] \ge 1 - B$$

$\left|\sum_{i=1}^{\ell} r_i e_i\right| \le \sum_{i=1}^{\ell} |r_i \cdot e_i|$; $|r_i \cdot e_i| \le |e_i|$ since $r_i \in \{0,1\}$; random sample

So, $\Pr[\text{decryption failure}] \le B$

computed in part 1.

Remark: $x \ge B \iff -x \le -B \iff 1 - x \le 1 - B$

② 1. Notice that $\overset{\text{integer}}{b_i} = s \cdot \overset{\text{vector}}{a_i} + e_i = s \cdot a_i$ when $e_i = 0$. Then we can write $b = \begin{bmatrix} b_1 \\ \vdots \\ b_\ell \end{bmatrix}$, $A = \begin{bmatrix} - a_1 - \\ \vdots \\ - a_\ell - \end{bmatrix}$ and observe that $b = A \cdot s$.

By assumption $\ell >> n$, so we can solve this linear system using Gaussian elimination and get s. Once you have the secret key you can recover the message.

2. When $r_i = 1$ for all i, $c_1 = m\frac{(p-1)}{2} + \sum_{i=1}^{\ell} r_i \cdot b_i = m\frac{(p-1)}{2} + \sum_{i=1}^{\ell} b_i$. Since b_i's are known, we can compute $c_1 - \sum_{i=1}^{\ell} b_i = m\frac{(p-1)}{2} = \begin{cases} 0 & \text{if } m = 0, \\ \text{not } 0 & \text{if } m = 1. \end{cases}$

3. "$\Pr_{e \leftarrow P_\sigma}[e \neq 0 \bmod p] = \frac{1}{2\ell}$" can be interpreted as among ℓ-many samples of (a_i, b_i, e_i) only one of them will have a nonzero error e_i. Choosing some subset of these samples of size $> n$ and applying Gaussian elimination as in part 1 will give secret key with high probability. More precisely, as long as triples (a_i, b_i, e_i) where $e_i \neq 0$ are not included in the subset, Gaussian el. will work and s will be discovered.

③ 1. Note that in Regev's scheme, $\ell = 2$. (referring to the one in Ex. 3, not the parameter in Regev's Enc.) Similarly, decryption scheme can be written as $\mathrm{Dec}(s, (c_0, c_1)) = \left\lfloor (c_1 - s \cdot c_0) \frac{\ell}{p} \right\rceil = \left\lfloor \left(e + \left\lfloor \frac{m(p-1)}{\ell} \right\rceil\right) \frac{\ell}{p} \right\rceil$.

Decryption will be correct if $|e \cdot \frac{\ell}{p}| < \frac{1}{2}$, i.e., $|e| < \frac{p}{2\ell} =: \sigma$.

2. $\mathrm{Dec}(s, c'') = \mathrm{Dec}(s, (c_0'', c_1'')) = \mathrm{Dec}(s, (c_0 + c_0', c_1 + c_1')) = \left\lfloor ((c_1 + c_1') - s(c_0 + c_0')) \frac{\ell}{p} \right\rceil$.

$c_1 + c_1' = (a + a')s + (e + e') + \left\lfloor m \frac{(p-1)}{\ell} \right\rceil + \left\lfloor m' \frac{(p-1)}{\ell} \right\rceil$ and $c_0 + c_0' = a + a'$ implies

$$\left\lfloor ((c_1 + c_1') - s(c_0 + c_0')) \frac{\ell}{p} \right\rceil = \left\lfloor \left((e + e') + \left\lfloor m \frac{(p-1)}{\ell} \right\rceil + \left\lfloor m' \frac{(p-1)}{\ell} \right\rceil \right) \frac{\ell}{p} \right\rceil.$$

When $|(e + e')\frac{\ell}{p}| < \frac{1}{2}$, the decryption will give $m + m'$.