Supplementary Material

A Bounding the Probabilities of the Bad Events

A.1 Bounding badτ-switch

Let's first fix a pair of values for the indices i and j. If $j \in \mathcal{I}_{\mathsf{enc}}$, then the probability of the event $(S^j, T^j) = (S^i, T^i)$ comes out to be $(1/N) \cdot (1/N)$ due to the n-bit randomness over each of S^j and T^j. Similarly, if $j \in \mathcal{I}_{\mathsf{dec}}$, then the probability of the event $(L^j, R^j) = (L^i, R^i)$ comes out to be $(1/N) \cdot (1/N)$ due to the n-bit randomness over each of L^j and R^j. As we can choose the pair of indices (i, j) in $\binom{q}{2}$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\tau\text{-}\mathsf{switch}] \leq \frac{\binom{q}{2}}{N^2}. \tag{87}$$

A.2 Bounding badτ-$\widehat{Y}$

Let's first fix a pair of values for the indices i and j. If $j \in \mathcal{I}_{\mathsf{enc}}$, then the probability of each of the events $S^i = S^j$ and $L^i + T^i = L^j + T^j$ comes out to be $(1/N^2)$ due to the n- bit randomness over S^j and T^j respectively. Similarly if $j \in \mathcal{I}_{\mathsf{dec}}$, then the probability of each of the events $R^i = R^j$ and $L^i + T^i = L^j + T^j$ comes out to be $(1/N^2)$ due to the n- bit randomness over R^j and L^j respectively. As we can choose the pair of indices (i, j) in $\binom{q}{2}$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\tau\text{-}\widehat{Y}] \leq \frac{\binom{q}{2}}{N^2}. \tag{88}$$

A.3 Bounding badτ-3path

Proposition 4 *Having defined the bad event badτ-3path in Fig. 3, we have*

$$\Pr[\mathsf{bad}\tau\text{-}\mathsf{3path}] \leq \frac{\binom{q}{3}}{N^2}.$$

To prove the proposition, let's first fix three distinct values for the indices i, j and l. We'll study this bad event in the following four sub-cases.

- badτ-3path-1: If $j, l \in \mathcal{I}_{\mathsf{dec}}$, then $\Pr[R^i = R^j = R^l] = \Pr[R^i = R^j] \cdot \Pr[R^i = R^j = R^l | R^i = R^j]$ (as $\Pr[R^i = R^j = R^l | R^i \neq R^j] = 0$). This probability comes out to be $(1/N^2)$. The n-bit randomness for the first term on the RHS comes from R^j and the same randomness for the second term on the RHS comes from R^l.
- badτ-3path-2: If $j, l \in \mathcal{I}_{\mathsf{enc}}$, then $\Pr[S^i = S^j = S^l] = \Pr[S^i = S^j] \cdot \Pr[S^i = S^j = S^l | S^i = S^j]$ (as $\Pr[S^i = S^j = S^l | S^i \neq S^j] = 0$). This probability comes out to be $(1/N^2)$. The n-bit randomness for the first term on the RHS comes from S^j and the same randomness for the second term on the RHS comes from S^l.
- badτ-3path-3: If $j \in \mathcal{I}_{\mathsf{dec}}$ and $l \in \mathcal{I}_{\mathsf{enc}}$, then the probability of each of the events $R^i = R^j = R^l$ and $S^i = S^j = S^l$ comes out to be $(1/N)$. The n-bit randomness comes from R^j and S^l respectively.
- badτ-3path-4: If $j \in \mathcal{I}_{\mathsf{enc}}$ and $l \in \mathcal{I}_{\mathsf{dec}}$, then the probability of each of the events $R^i = R^j = R^l$ and $S^i = S^j = S^l$ comes out to be $(1/N)$. The n-bit randomness comes from R^l and S^j respectively.

As we can choose the 3-tuple of indices (i, j, l) in $\binom{q}{3}$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\tau\text{-}\mathsf{3path}] \leq \frac{\binom{q}{3}}{N^2}. \tag{89}$$

A.4 Bounding badτ-3coll

Once we fix three distinct values for the indices i, j and l, the analysis of this bad event exactly corresponds to the first two sub-cases of the previous bad event(e.g., badτ-3path). As we can choose the 3-tuple of indices (i, j, l) in $\binom{q}{3}$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\tau\text{-}\mathsf{3coll}] \leq \frac{\binom{q}{3}}{N^2}. \tag{90}$$

A.5 Bounding badK-outer

Proposition 5 *Having defined the bad event badK-outer in Fig. 4, we have*

$$\Pr[\mathsf{badK\text{-}outer}] \leq \frac{qq_1q_5 + q^2(q_1 + q_5)}{N^2}.$$

To prove this proposition, we note that this bad event occurs when one of the following happens. Note that the event $\mathcal{I}_{RR} \cap \mathcal{I}_{SS} \neq \emptyset$ is an impossible event as $\mathcal{I}_{RR} \subseteq \mathcal{I}_{\mathsf{dec}}$ and $\mathcal{I}_{SS} \subseteq \mathcal{I}_{\mathsf{enc}}$ from definition.

- badK-outer-1 $\mathcal{I}_R \cap \mathcal{I}_S \neq \emptyset$. This bad event occurs when for some $i \in [q]$, $j \in [q_1]$ and $l \in [q_5]$, $R^i + K_1 = U_1^j$ and $S^i + K_5 = U_5^l$. Let's first fix the values for the indices i, j and l. Then the probability of each of the events $R^i + K_1 = U_1^j$ and $S^i + K_5 = U_5^l$ comes out to be $(1/N)$. The n-bit randomness comes from the keys K_1 and K_5 respectively. As we can choose the indices i, j and l in q, q_1 and q_5 ways respectively, we use the union bound over all those possible choices to obtain
$$\Pr[\mathcal{I}_R \cap \mathcal{I}_S \neq \emptyset] \leq \frac{qq_1q_5}{N^2}. \tag{91}$$
- badK-outer-2 $\mathcal{I}_R \cap \mathcal{I}_{RR} \neq \emptyset$. This bad event occurs when for some $i \in \mathcal{I}_{\mathsf{dec}}$, $j \in [q_1]$ and $l \in [i-1]$, $R^i + K_1 = U_1^j$ and $R^i = R^l$. Let's first fix the values for the indices i, j and l. The probability of the event $R^i + K_1 = U_1^j$ comes out to be $(1/N)$. The n-bit randomness comes from the key K_1. The probability of the event $R^i = R^l$ also comes out to be $(1/N)$. The n-bit randomness comes from R^i as $i > l$ and $i \in \mathcal{I}_{\mathsf{dec}}$. As we can choose the pair of indices (i, l) in $\binom{q}{2}$ ways and the index j in q_1 ways, we use the union bound over all those possible choices to obtain
$$\Pr[\mathcal{I}_R \cap \mathcal{I}_{RR} \neq \emptyset] \leq \frac{q_1\binom{q}{2}}{N^2}. \tag{92}$$
- badK-outer-3 $\mathcal{I}_S \cap \mathcal{I}_{SS} \neq \emptyset$. This bad event occurs when for some $i \in \mathcal{I}_{\mathsf{enc}}$, $j \in [q_5]$ and $l \in [i-1]$, $S^i + K_5 = U_5^j$ and $S^i = S^l$. Let's first fix the values for the indices i, j and l. The probability of the event $S^i + K_5 = U_5^j$ comes out to be $(1/N)$. The n-bit randomness comes from the key K_5. The probability of the event $S^i = S^l$ also comes

out to be $(1/N)$. The n-bit randomness comes from S^i as $i > l$ and $i \in \mathcal{I}_{\mathsf{enc}}$. As we can choose the pair of indices (i,l) in $\binom{q}{2}$ ways and the index j in q_5 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathcal{I}_S \cap \mathcal{I}_{SS} \neq \emptyset] \leq \frac{q_5\binom{q}{2}}{N^2}\,. \tag{93}$$

– badK-outer-4 $\mathcal{I}_R \cap \mathcal{I}_{SS} \neq \emptyset$. This bad event occurs when for some $i \in \mathcal{I}_{\mathsf{enc}}$, $j \in [q_1]$ and $l \in [i-1]$, $R^i + K_1 = U_1^j$ and $S^i = S^l$. Let's first fix the values for the indices i, j and l. The probability of the event $R^i + K_1 = U_1^j$ comes out to be $(1/N)$. The n-bit randomness comes from the key K_1. The probability of the event $S^i = S^l$ also comes out to be $(1/N)$. The n-bit randomness comes from S^i as $i > l$ and $i \in \mathcal{I}_{\mathsf{enc}}$. As we can choose the pair of indices (i,l) in $\binom{q}{2}$ ways and the index j in q_1 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathcal{I}_S \cap \mathcal{I}_{SS} \neq \emptyset] \leq \frac{q_1\binom{q}{2}}{N^2}\,. \tag{94}$$

– badK-outer-5 $\mathcal{I}_S \cap \mathcal{I}_{RR} \neq \emptyset$. This bad event occurs when for some $i \in \mathcal{I}_{\mathsf{dec}}$, $j \in [q_5]$ and $l \in [i-1]$, $S^i + K_5 = U_5^j$ and $R^i = R^l$. Let's first fix the values for the indices i, j and l. The probability of the event $S^i + K_5 = U_5^j$ comes out to be $(1/N)$. The n-bit randomness comes from the key K_5. The probability of the event $R^i = R^l$ also comes out to be $(1/N)$. The n-bit randomness comes from R^i as $i > l$ and $i \in \mathcal{I}_{\mathsf{dec}}$. As we can choose the pair of indices (i,l) in $\binom{q}{2}$ ways and the index j in q_5 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathcal{I}_R \cap \mathcal{I}_{RR} \neq \emptyset] \leq \frac{q_5\binom{q}{2}}{N^2}\,. \tag{95}$$

Adding the probabilities of all these sub-cases, we obtain

$$\Pr[\mathsf{badK\text{-}outer}] \leq \frac{qq_1q_5 + q^2(q_1+q_5)}{N^2}\,. \tag{96}$$

A.6 Bounding badK-source

Proposition 6 *Having defined the bad event badK-source in Fig. 4, we have*

$$\Pr[\mathit{badK\text{-}source}] \leq \frac{(q_1+q_5)\binom{q}{2} + 2\binom{q}{3}}{N^2}.$$

This bad event occurs when one of the following happens.

– badK-source1. $\exists i \in \mathcal{I}_S$, $j \in \mathcal{I}_{RR}, i < j$ and $R^i = R^j$. In other words, $\exists i \in [q]$ and $j \in \mathcal{I}_{\mathsf{dec}}$ with $i < j$ and $l \in [q_5]$ such that $S^i + K_5 = U_5^l$ and $R^i = R^j$. Let's first fix the values for the indices i, j and l. The probability of each of the events $S^i + K_5 = U_5^l$ and $R^i = R^j$ comes out to be $(1/N)$. The n-bit randomness comes from the key K_5 and R_j respectively. As we can choose the pair of indices (i,j) in $\binom{q}{2}$ ways and the index l in q_5 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{badK\text{-}source1}] \leq \frac{q_5\binom{q}{2}}{N^2}\,. \tag{97}$$

– badK-source2. $\exists i \in \mathcal{I}_{SS}, j \in \mathcal{I}_{RR}, i < j$ and $R^i = R^j$. In other words, $\exists l \in [q], i \in \mathcal{I}_{\mathsf{enc}}$ and $j \in \mathcal{I}_{\mathsf{dec}}$ with $k < i < j$ such that $R^i = R^j$ and $S^i = S^k$. Let's first fix the values for the indices i, j and l. The probability of each of the events $R^i = R^j$ and $S^i = S^k$ comes out to be $(1/N)$. The n-bit randomness comes from R_j and S_i respectively. As we can choose the 3-tuple of indices (i, j, l) in $\binom{q}{3}$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{badK-source2}] \leq \frac{\binom{q}{3}}{N^2}. \tag{98}$$

– badK-source3. $\exists i \in \mathcal{I}_R, j \in \mathcal{I}_{SS}, i < j$ and $S^i = S^j$. In other words, $\exists i \in [q]$ and $j \in \mathcal{I}_{\mathsf{enc}}$ with $i < j$ and $l \in [q_1]$ such that $R^i + K_1 = U_1^l$ and $S^i = S^j$. Let's first fix the values for the indices i, j and l. The probability of each of the events $R^i + K_1 = U_1^l$ and $S^i = S^j$ comes out to be $(1/N)$. The n-bit randomness comes from the key K_1 and S_j respectively. As we can choose the pair of indices (i, j) in $\binom{q}{2}$ ways and the index l in q_1 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{badK-source3}] \leq \frac{q_1\binom{q}{2}}{N^2}. \tag{99}$$

– badK-source4. $\exists i \in \mathcal{I}_{RR}, j \in \mathcal{I}_{SS}, i < j$ and $S^i = S^j$. In other words, $\exists l \in [q], i \in \mathcal{I}_{\mathsf{dec}}$ and $j \in \mathcal{I}_{\mathsf{enc}}$ with $k < i < j$ such that $S^i = S^j$ and $R^i = R^k$. Let's first fix the values for the indices i, j and l. The probability of each of the events $S^i = S^j$ and $R^i = R^k$ comes out to be $(1/N)$. The n-bit randomness comes from S_j and R_i respectively. As we can choose the 3-tuple of indices (i, j, l) in $\binom{q}{3}$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{badK-source4}] \leq \frac{\binom{q}{3}}{N^2}. \tag{100}$$

Adding the probabilities of all these sub-cases, we obtain

$$\Pr[\text{badK-source}] \leq \frac{(q_1 + q_5)\binom{q}{2} + 2\binom{q}{3}}{N^2}. \tag{101}$$

A.7 Bounding badμ-in&out

Proposition 7 *Having defined the bad event badμ-in&out in Fig. 7, we have*

$$\Pr[\textit{bad}\mu\textit{-in\&out}] \leq \frac{q^2(3q_1 + 3q_5 + q_2 + q_3 + q_4)}{N^2} + \frac{5q^3}{N^2} + \frac{qq_1(q_3 + q_4 + q_5)}{N^2}$$
$$+ \frac{qq_5(q_2 + q_3 + q_4)}{N^2} + \frac{2q^2q_1q_5}{N^3} + \frac{2q^3(q_1 + q_5)}{N^3} + \frac{2q^2}{N^2}.$$

This bad event occurs when $(\mathcal{I}_R \sqcup \mathcal{I}_S \sqcup \mathcal{I}_{RR} \sqcup \mathcal{I}_{SS}) \cap (\mathcal{I}_X \cup \mathcal{I}_{XX} \cup \mathcal{I}_{\widehat{Y}} \cup \mathcal{I}_{\widehat{Y}\widehat{Y}} \cup \mathcal{I}_Z \cup \mathcal{I}_{ZZ}) \neq \emptyset$. Note that, by definition $\mathcal{I}_R \cap \mathcal{I}_{XX} = \emptyset$ and $\mathcal{I}_S \cap \mathcal{I}_{ZZ} = \emptyset$. We individually bound each of the bad events as follows:

– badμ-in&out-1. $\mathcal{I}_R \cap \mathcal{I}_X \neq \emptyset$. This bad event occurs when $\exists i \in [q], j \in [q_1]$ and $l \in [q_5]$ such that $R^i + K_1 = U_1^j$ and $X^i + K_2 = U_2^l$. Let's first fix the values for the indices i, j and l. The probability of each of the events $R^i + K_1 = U_1^j$ and $X^i + K_2 = U_2^l$ comes out to be $(1/N)$ due to the n-bit randomness over the keys K_1 and K_2 respectively. As we can choose the indices i, j and l in q, q_1 and q_5 ways respectively, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-1}] \leq \frac{qq_1q_5}{N^2}. \tag{102}$$

– badμ-in&out-2. $\mathcal{I}_{RR} \cap \mathcal{I}_X \neq \emptyset$. This bad event occurs when $\exists i \in \mathcal{I}_{\mathsf{dec}}, j \in [i-1]$ and $l \in [q_2]$ such that $R^i = R^j$ and $X^i + K_2 = U_2^l$. Let's first fix the values for the indices i, j and l. The probability of each of the events $R^i = R^j$ and $X^j + K_2 = U_2^l$ comes out to be $(1/N)$ due to the n-bit randomness over R^i and K_2 respectively. As we can choose the pair of indices (i,j) in $\binom{q}{2}$ ways and the index l in q_2 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-2}] \leq \frac{q_2\binom{q}{2}}{N^2}. \tag{103}$$

– badμ-in&out-3. $\mathcal{I}_{RR} \cap \mathcal{I}_{XX} \neq \emptyset$. This bad event occurs when $\exists i \in \mathcal{I}_{\mathsf{dec}}, j \in [i-1]$, and $l \in [q]$ with $i \neq l$ such that $R^i = R^j$ and $X^i = X^l$, which we equivalently write as

$$R^i = R^j, \widehat{R}^i + \widehat{R}^l = L^i + L^l.$$

We analyze this event into two separate subcases: (a) when $l = j$ and if j is a decryption query, then, the above event boils down to the event $R^i = R^j, L^i = L^j$, which triggers the bad event badτ-switch. Therefore, we analyse the case (b) when $l \neq j$. In this case, we use the randomness of R^i and $\widehat{R}^i$ to bound the above event to at most $(2/N^2)$ As we can choose the pair of indices $\{i,j\}$ in $\binom{q}{2}$ ways and for each of those choices, we can choose the index l in $(q-1)$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-3}] \leq \frac{q^3}{N^2}. \tag{104}$$

– badμ-in&out-4. $\mathcal{I}_R \cap \mathcal{I}_{\widehat{Y}} \neq \emptyset$. This bad event occurs when $\exists i \in [q], j \in [q_1]$ and $k \in [q_3]$ such that $R^i + K_1 = U_1^j$ and $\widehat{Y}^i + K_3 = V_3^k$, which we equivalently write as

$$R^i + K_1 = U_1^j, \widehat{R}^i + L^i + \widehat{S}^i + T^i + K_3 = V_3^k.$$

For a fixed choice of indices, the probability of the event is at most $1/N^2$ due to the n-bit randomness over K_1 and K_3. We can choose the triplet of indices (i,j,k) is at most qq_1q_3 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-4}] \leq \frac{qq_1q_3}{N^2}. \tag{105}$$

– badμ-in&out-5. $\mathcal{I}_R \cap \mathcal{I}_{\widehat{Y}\widehat{Y}} \neq \emptyset$. This bad event occurs when $\exists i \in [q], j \in [q]$ and $k \in [q_1]$ such that $R^i + K_1 = U_1^k$ and $\widehat{Y}^i = \widehat{Y}^j$, which we equivalently write as

$$R^i + K_1 = U_1^k, \widehat{R}^i + \widehat{S}^i + \widehat{R}^j + \widehat{S}^j = L^i + L^j + T^i + T^j.$$

For a fixed choice of indices, the probability of the event is at most $2/N^2$ due to the n-bit randomness over K_1 and the n-bit randomness over $\widehat{S}^i$ (note that $i \notin \mathcal{I}_S$ and $i \notin \mathcal{I}_{SS}$). As we can choose the pair of indices $\{i,j\}$ in $\binom{q}{2}$ ways and for each of those choices, we can choose the index k in q_1 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-5}] \leq \frac{q^2q_1}{N^2}. \tag{106}$$

– badμ-in&out-6. $\mathcal{I}_R \cap \mathcal{I}_Z \neq \emptyset$. This bad event occurs when $\exists i \in [q], j \in [q_1]$ and $k \in [q_4]$ such that $R^i + K_1 = U_1^j$ and $Z^i + K_4 = U_4^k$, which we equivalently write as

$$R^i + K_1 = U_1^j, \widehat{S}^i + T^i + K_4 = U_4^k.$$

For a fixed choice of indices, the probability of the event is at most $1/N^2$ due to the n-bit randomness over K_1 and K_4. However, the total number of choices of the indices is at most qq_1q_4, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-6}] \leq \frac{qq_1q_4}{N^2}. \tag{107}$$

- badμ-in&out-7. $\mathcal{I}_R \cap \mathcal{I}_{ZZ} \neq \emptyset$. This bad event occurs when $\exists i \in [q], j \in [q]$ and $k \in [q_1]$ such that $R^i + K_1 = U_1^k$ and $Z^i = Z^j$, which we equivalently write as

$$R^i + K_1 = U_1^k, \widehat{S}^i + T^i = \widehat{S}^j + T_j.$$

For a fixed choice of indices, the probability of the event is at most $2/N^2$ due to the n-bit randomness over K_1 and $\widehat{S}^i$ (note that $\widehat{S}^i$ is freshly sampled as $i \notin \mathcal{I}_S$ and $i \notin \mathcal{I}_{SS}$). However, the total number of choices of the indices is at most $\binom{q}{2}q_1$, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-7}] \leq \frac{q^2 q_1}{N^2}. \tag{108}$$

- badμ-in&out-8. $\mathcal{I}_S \cap \mathcal{I}_X \neq \emptyset$. Analysis of this case is similar to that of badμ-in&out-1., where we use the randomness of K_5 and K_2. Looking ahead, we bound the probability to be at most

$$\Pr[\text{bad}\mu\text{-in\&out-8}] \leq \frac{q q_2 q_5}{N^2}. \tag{109}$$

- badμ-in&out-9. $\mathcal{I}_S \cap \mathcal{I}_{XX} \neq \emptyset$. Analysis of this case is again similar to that of badμ-in&out-7., where we use the randomness of K_5 and $\widehat{R}^i$. Looking ahead, we bound the probability to be at most

$$\Pr[\text{bad}\mu\text{-in\&out-9}] \leq \frac{q^2 q_5}{N^2}. \tag{110}$$

- badμ-in&out-10. $\mathcal{I}_S \cap \mathcal{I}_{\widehat{Y}} \neq \emptyset$. Analysis of this case is again similar to that of badμ-in&out-4., where we use the randomness of K_5 and K_3. Looking ahead, we bound the probability to be at most

$$\Pr[\text{bad}\mu\text{-in\&out-10}] \leq \frac{q q_3 q_5}{N^2}. \tag{111}$$

- badμ-in&out-11. $\mathcal{I}_S \cap \mathcal{I}_{\widehat{Y}\widehat{Y}} \neq \emptyset$. Analysis of this case is again similar to that of badμ-in&out-5., where we use the randomness of K_5 and $\widehat{R}^i$. Looking ahead, we bound the probability to be at most

$$\Pr[\text{bad}\mu\text{-in\&out-11}] \leq \frac{q^2 q_5}{N^2}. \tag{112}$$

- badμ-in&out-12. $\mathcal{I}_S \cap \mathcal{I}_Z \neq \emptyset$. Analysis of this case is again similar to that of badμ-in&out-6., where we use the randomness of K_5 and K_4. Looking ahead, we bound the probability to be at most

$$\Pr[\text{bad}\mu\text{-in\&out-12}] \leq \frac{q q_4 q_5}{N^2}. \tag{113}$$

- badμ-in&out-13. $\mathcal{I}_{RR} \cap \mathcal{I}_{\widehat{Y}} \neq \emptyset$. This bad event occurs when $\exists i \in \mathcal{I}_{\mathsf{dec}}, j \in [i-1]$ and $k \in [q_3]$ such that $R^i = R^j$ and $\widehat{Y}^i + K_3 = V_3^k$, which we equivalently write as

$$R^i = R^j, \widehat{R}^i + L^i + \widehat{S}^i + T^i + K_3 = V_3^k.$$

For a fixed choice of indices, the probability of the event is at most $1/N^2$ due to the n-bit randomness over R^i and K_3. We can choose the triplet of indices (i, j, k) is at most $\binom{q}{2}q_3$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-13}] \leq \frac{q^2 q_3}{2N^2}. \tag{114}$$

– badμ-in&out-14. $\mathcal{I}_{RR} \cap \mathcal{I}_{\widehat{Y}\widehat{Y}} \neq \emptyset$. This bad event occurs when $\exists i \in \mathcal{I}_{\mathsf{dec}}, j \in [i-1]$ and $k \in [q]$ such that $R^i = R^j$ and $\widehat{Y}^i = \widehat{Y}^k$, which we equivalently write as

$$R^i = R^j, \widehat{R}^i + \widehat{S}^i + \widehat{R}^k + \widehat{S}^k = L^i + L^k + T^i + T^k.$$

Now, we consider two separate subcases: (i) if $k = j$ and it is a decryption query, then the above event boils down to $R^i = R^j, L^i + L^j = T^i + T^j$ (assuming in both of the decryption queries S values are same). Then, using the randomness of R^i and L^i, we bound the above probability to be at most $1/N^2$. Moreover, the number of choices for (i, j) to be at most $\binom{q}{2}$. Therefore, by using the union bound, the probability of the above event is at most $q^2/2N^2$.

Now, we consider the other case when $k \neq j$. In this case, we use the randomness of R^i and $\widehat{R}^i$ to bound the above event to at most $2/N^2$. The number of choices for triplets (i, j, k) is q^3. Therefore, by using the union bound, the probability of the above event is at most q^3/N^2.

Combining the above two cases, we obtain

$$\Pr[\text{bad}\mu\text{-in\&out-14}] \leq \frac{q^2}{2N^2} + \frac{q^3}{N^2}. \tag{115}$$

– badμ-in&out-15. $\mathcal{I}_{RR} \cap \mathcal{I}_{Z} \neq \emptyset$. This bad event occurs when $\exists i \in \mathcal{I}_{\mathsf{dec}}, j \in [i-1]$ and $k \in [q_4]$ such that $R^i = R^j$ and $Z^i + K_4 = U_4^k$, which we equivalently write as

$$R^i = R^j, \widehat{S}^i + T^i + K_4 = U_4^k.$$

For a fixed choice of indices, the probability of the event is at most $1/N^2$ due to the n-bit randomness over R^i and K_4. However, the total number of choices of the indices is at most $\binom{q}{2} q_4$, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-15}] \leq \frac{q^2 q_4}{2N^2}. \tag{116}$$

– badμ-in&out-16. $\mathcal{I}_{RR} \cap \mathcal{I}_{ZZ} \neq \emptyset$. This bad event occurs when $\exists i \in \mathcal{I}_{\mathsf{dec}}, j \in [i-1]$ and $k \in [q]$ such that $R^i = R^j$ and $Z^i = Z^k$, which we equivalently write as

$$R^i = R^j, \widehat{S}^i + T^i = \widehat{S}^k + T^k.$$

For a fixed choice of indices, the probability of the event is at most $2/N^2$ due to the n-bit randomness over $\widehat{R}^i$ and $\widehat{S}^i$ (note that $\widehat{S}^i$ is freshly sampled as $S^i \neq S^j$ and $i \notin \mathcal{I}_S$). However, the total number of choices of the indices is at most $\binom{q}{2} q$, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-16}] \leq \frac{q^3}{2N^2}. \tag{117}$$

– badμ-in&out-17. $\mathcal{I}_{SS} \cap \mathcal{I}_{X} \neq \emptyset$. Analysis of this bad event is similar to that of badμ-in&out-12, where we use the randomness of S^i and K_2. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\mu\text{-in\&out-17}] \leq \frac{q_2 \binom{q}{2}}{N^2}. \tag{118}$$

– badμ-in&out-18. $\mathcal{I}_{SS} \cap \mathcal{I}_{XX} \neq \emptyset$. This bad event occurs when $\exists i \in \mathcal{I}_{\mathsf{enc}}, j \in [i-1]$, and $l \in [q]$ with $i \neq l$ such that $S^i = S^j$ and $X^i = X^l$, which we equivalently write as

$$S^i = S^j, \widehat{R}^i + \widehat{R}^l = L^i + L^l.$$

We use the randomness of S^i and $\widehat{R}^i$ to bound the above event to at most $(2/N^2)$ As we can choose the pair of indices $\{i, j\}$ in $\binom{q}{2}$ ways and for each of those choices, we can choose the index l in $(q-1)$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-in\&out-18}] \leq \frac{q^3}{N^2}. \tag{119}$$

- badμ-in&out-19. $\mathcal{I}_{SS} \cap \mathcal{I}_{\widehat{Y}} \neq \emptyset$. Analysis of this bad event is similar to that of badμ-in&out-13, where we use the randomness of S^i and K_3. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\mu\text{-in\&out-19}] \leq \frac{q^2 q_3}{2N^2}. \tag{120}$$

- badμ-in&out-20. $\mathcal{I}_{SS} \cap \mathcal{I}_{\widehat{Y}\widehat{Y}} \neq \emptyset$. Analysis of this bad event is similar to that of badμ-in&out-16, where we use the randomness of S^i instead of R^i, wherever applicable. Looking ahead, we bound the probability of the above event to at most

$$\Pr[\text{bad}\mu\text{-in\&out-20}] \leq \frac{q^2}{2N^2} + \frac{q^3}{N^2}. \tag{121}$$

- badμ-in&out-21. $\mathcal{I}_{SS} \cap \mathcal{I}_{Z} \neq \emptyset$. Analysis of this bad event is similar to that of badμ-in&out-15, where we use the randomness of S^i and K_4. Looking ahead, we bound the above event to at most

$$\Pr[\text{bad}\mu\text{-in\&out-21}] \leq \frac{q^2 q_4}{2N^2}. \tag{122}$$

- badμ-in&out-22. $\mathcal{I}_{SS} \cap \mathcal{I}_{ZZ} \neq \emptyset$. Again, the analysis of this bad event is similar to that of badμ-in&out-3, where we use the randomness of S^i, wherever applicable. Looking ahead, we bound the above probability to be at most

$$\Pr[\text{bad}\mu\text{-in\&out-22}] \leq \frac{q^3}{2N^2}. \tag{123}$$

By combining Eqn. (102)-Eqn. (123), we obtain

$$\begin{aligned}\Pr[\text{bad}\mu\text{-in\&out}] \leq & \frac{q^2(2q_1 + 2q_5 + q_2 + q_3 + q_4)}{N^2} + \frac{5q^3}{N^2} + \frac{qq_1(q_3 + q_4 + q_5)}{N^2} \\ & + \frac{qq_5(q_2 + q_3 + q_4)}{N^2} + \frac{2q^2}{N^2}. \end{aligned} \tag{124}$$

A.8 Bounding badμ-source

Proposition 8 *Having defined the bad event badμ-source in Fig. 7, we have*

$$\Pr[\text{bad}\mu\text{-source}] \leq \frac{2\binom{q}{2}(q_1 + q_5)}{N^2}.$$

To prove the proposition, we first fix the values for the indices i, j and l.

- badμ-source-1. $i, j \in [q]$ with $i \neq j$ and $l \in [q_1]$ such that $R^i + K_1 = U_1^l$ and $\widehat{R}^i + \widehat{R}^j = L^i + L^j$. The probability of the event $R^i + K_1 = U_1^l$ comes out to be $(1/N)$ due to the randomness over the key K_1. The probability of the event $\widehat{R}^i + \widehat{R}^j = L^i + L^j$ comes out to be at most $(2/N)$ due to the randomness over $\widehat{R}^j$.

- badμ-source-2. $i, j \in [q]$ with $i \neq j$ and $l \in [q_5]$ such that $S^i + K_5 = U_5^l$ and $\widehat{S}^i + \widehat{S}^j = T^i + T^j$. The probability of the event $S^i + K_5 = U_5^l$ comes out to be $(1/N)$ due to the randomness over the key K_5. The probability of the event $\widehat{S}^i + \widehat{S}^j = T^i + T^j$ comes out to be at most $(2/N)$ due to the randomness over $\widehat{S}^j$.

As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ ways and the index l in q_1 or q_5 ways (for badμ-source-1 and badμ-source-2 respectively), we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-source}] \leq \frac{2\binom{q}{2}(q_1 + q_5)}{N^2}. \tag{125}$$

A.9 Bounding badμ-inner

Proposition 9 *Having defined the bad event badμ-inner in Fig. 7, we have*

$$\Pr[\text{bad}\mu\text{-inner}] \leq \frac{q(q_2q_3 + q_3q_4 + q_1q_4)}{N^2} + \frac{3q^2(q_2 + q_3 + q_4)}{N^2} + \frac{3q^3}{N^2}.$$

This bad event occurs when one of the following happens.

- badμ-inner-1. $\mathcal{I}_X \cap \mathcal{I}_{\widehat{Y}} \neq \emptyset$. This bad event occurs when $\exists i \in [q]$, $j \in [q_2]$ and $l \in [q_3]$ such that $X^i + K_2 = U_2^j$ and $\widehat{Y}^i + K_3 = V_3^l$. Let's first fix the values for the indices i, j and l. The probability of each of the events $X^i + K_2 = U_2^j$ and $\widehat{Y}^l = V_3^l$ comes out to be $(1/N)$ due to the randomness over the keys K_2 and K_3 respectively. As we can choose the indices i, j and l in q, q_2 and q_3 ways respectively, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-1}] \leq \frac{qq_2q_3}{N^2}\,. \tag{126}$$

- badμ-inner-2. $\mathcal{I}_{\widehat{Y}} \cap \mathcal{I}_Z \neq \emptyset$. This bad event occurs when $\exists i \in [q]$, $j \in [q_3]$ and $l \in [q_4]$ such that $\widehat{Y}^i + K_3 = V_3^j$ and $Z^i + K_4 = U_3^l$. Let's first fix the values for the indices i, j and l. The probability of each of the events $\widehat{Y}^i + K_3 = V_3^j$ and $Z^i + K_4 = U_3^l$ comes out to be $(1/N)$ due to the randomness over the keys K_3 and K_4 respectively. As we can choose the indices i, j and l in q, q_3 and q_4 ways respectively, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-2}] \leq \frac{qq_3q_4}{N^2}\,. \tag{127}$$

- badμ-inner-3. $\mathcal{I}_Z \cap \mathcal{I}_X \neq \emptyset$. This bad event occurs when $\exists i \in [q]$, $j \in [q_4]$ and $l \in [q_1]$ such that $Z^i + K_4 = U_4^j$ and $X^i + K_1 = U_1^l$. Let's first fix the values for the indices i, j and l. The probability of each of the events $Z^i + K_4 = U_4^j$ and $X^i + K_1 = U_1^l$ comes out to be $(1/N)$ due to the randomness over the keys K_4 and K_1 respectively. As we can choose the indices i, j and l in q, q_4 and q_1 ways respectively, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-3}] \leq \frac{qq_4q_1}{N^2}\,. \tag{128}$$

- badμ-inner-4. $\mathcal{I}_X \cap \mathcal{I}_{XX} \neq \emptyset$. This bad event occurs when $\exists i, j \in [q]$ with $i \neq j$ and $l \in [q_2]$ such that $X^i + K_2 = U_2^l$ and $X^i = X^j$. Let's first fix the values for the indices i, j and l. The probability of the event $X^i + K_2 = U_2^l$ comes out to be $(1/N)$ due to the randomness over the key K_2. The probability of the event $X^i = X^j$ comes out to be at most $(2/N)$ due to the n-bit randomness over X^i or X^j. As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ and l in q_2 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-4}] \leq \frac{2q_2\binom{q}{2}}{N^2}\,. \tag{129}$$

- badμ-inner-5. $\mathcal{I}_X \cap \mathcal{I}_{\widehat{Y}\widehat{Y}} \neq \emptyset$. This bad event occurs when $\exists i, j \in [q]$ with $i \neq j$ and $l \in [q_2]$ such that $X^i + K_2 = U_2^l$ and $\widehat{Y}^i = \widehat{Y}^j$. Let's first fix the values for the indices i, j and l. The probability of the event $X^i + K_2 = U_2^l$ comes out to be $(1/N)$ due to the randomness over the key K_2. The probability of the event $\widehat{Y}^i = \widehat{Y}^j$ comes out to be at most $(2/N)$ due to the n-bit randomness over $\widehat{Y}^i$ or $\widehat{Y}^j$. As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ and l in q_2 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-5}] \leq \frac{2q_2\binom{q}{2}}{N^2}\,. \tag{130}$$

– badμ-inner-6. $\mathcal{I}_X \cap \mathcal{I}_{ZZ} \neq \emptyset$. This bad event occurs when $\exists i, j \in [q]$ with $i \neq j$ and $l \in [q_2]$ such that $X^i + K_2 = U_2^l$ and $Z^i = Z^j$. Let's first fix the values for the indices i, j and l. The probability of the event $X^i + K_2 = U_2^l$ comes out to be $(1/N)$ due to the randomness over the key K_2. The probability of the event $Z^i = Z^j$ comes out to be at most $(2/N)$ due to the n-bit randomness over Z^i or Z^j. As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ and l in q_2 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-6}] \leq \frac{2q_2\binom{q}{2}}{N^2} . \quad (131)$$

– badμ-inner-7. $\mathcal{I}_{\widehat{Y}} \cap \mathcal{I}_{XX} \neq \emptyset$. This bad event occurs when $\exists i, j \in [q]$ with $i \neq j$ and $l \in [q_3]$ such that $\widehat{Y}^i + K_3 = U_3^l$ and $X^i = X^j$. Let's first fix the values for the indices i, j and l. The probability of the event $\widehat{Y}^i + K_3 = U_3^l$ comes out to be $(1/N)$ due to the randomness over the key K_3. The probability of the event $X^i = X^j$ comes out to be at most $(2/N)$ due to the n-bit randomness over X^i or X^j. As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ and l in q_3 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-7}] \leq \frac{2q_3\binom{q}{2}}{N^2} . \quad (132)$$

– badμ-inner-8. $\mathcal{I}_{\widehat{Y}} \cap \mathcal{I}_{\widehat{Y}\widehat{Y}} \neq \emptyset$. This bad event occurs when $\exists i, j \in [q]$ with $i \neq j$ and $l \in [q_3]$ such that $\widehat{Y}^i + K_3 = U_3^l$ and $\widehat{Y}^i = \widehat{Y}^j$. Let's first fix the values for the indices i, j and l. The probability of the event $\widehat{Y}^i + K_3 = U_3^l$ comes out to be $(1/N)$ due to the randomness over the key K_3. The probability of the event $\widehat{Y}^i = \widehat{Y}^j$ comes out to be at most $(2/N)$ due to the n-bit randomness over $\widehat{Y}^i$ or $\widehat{Y}^j$. As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ and l in q_3 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-8}] \leq \frac{2q_3\binom{q}{2}}{N^2} . \quad (133)$$

– badμ-inner-9. $\mathcal{I}_{\widehat{Y}} \cap \mathcal{I}_{ZZ} \neq \emptyset$. This bad event occurs when $\exists i, j \in [q]$ with $i \neq j$ and $l \in [q_3]$ such that $\widehat{Y}^i + K_3 = U_3^l$ and $Z^i = Z^j$. Let's first fix the values for the indices i, j and l. The probability of the event $\widehat{Y}^i + K_3 = U_3^l$ comes out to be $(1/N)$ due to the randomness over the key K_3. The probability of the event $Z^i = Z^j$ comes out to be at most $(2/N)$ due to the n-bit randomness over Z^i or Z^j. As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ and l in q_3 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-9}] \leq \frac{2q_3\binom{q}{2}}{N^2} . \quad (134)$$

– badμ-inner-10. $\mathcal{I}_Z \cap \mathcal{I}_{XX} \neq \emptyset$. This bad event occurs when $\exists i, j \in [q]$ with $i \neq j$ and $l \in [q_4]$ such that $Z^i + K_4 = U_4^l$ and $X^i = X^j$. Let's first fix the values for the indices i, j and l. The probability of the event $Z^i + K_4 = U_4^l$ comes out to be $(1/N)$ due to the randomness over the key K_4. The probability of the event $X^i = X^j$ comes out to be at most $(2/N)$ due to the n-bit randomness over X^i or X^j. As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ and l in q_4 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-10}] \leq \frac{2q_4\binom{q}{2}}{N^2} . \quad (135)$$

– badμ-inner-11. $\mathcal{I}_Z \cap \mathcal{I}_{\widehat{Y}\widehat{Y}} \neq \emptyset$. This bad event occurs when $\exists i, j \in [q]$ with $i \neq j$ and $l \in [q_4]$ such that $Z^i + K_4 = U_4^l$ and $\widehat{Y}^i = \widehat{Y}^j$. Let's first fix the values for the indices i, j and l. The probability of the event $Z^i + K_4 = U_4^l$ comes out to be $(1/N)$ due to the randomness over the key K_4. The probability of the event $\widehat{Y}^i = \widehat{Y}^j$ comes out to be at most $(2/N)$ due to the n-bit randomness over $\widehat{Y}^i$ or $\widehat{Y}^j$. As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ and l in q_4 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-11}] \leq \frac{2q_4\binom{q}{2}}{N^2}\,. \tag{136}$$

– badμ-inner-12. $\mathcal{I}_Z \cap \mathcal{I}_{ZZ} \neq \emptyset$. This bad event occurs when $\exists i, j \in [q]$ with $i \neq j$ and $l \in [q_4]$ such that $Z^i + K_4 = U_4^l$ and $Z^i = Z^j$. Let's first fix the values for the indices i, j and l. The probability of the event $Z^i + K_4 = U_4^l$ comes out to be $(1/N)$ due to the randomness over the key K_4. The probability of the event $Z^i = Z^j$ comes out to be at most $(2/N)$ due to the n-bit randomness over Z^i or Z^j. As we can choose the pair of indices (i, j) in $2\binom{q}{2}$ and l in q_4 ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-12}] \leq \frac{2q_4\binom{q}{2}}{N^2}\,. \tag{137}$$

– badμ-inner-13. $\mathcal{I}_{XX} \cap \mathcal{I}_{\widehat{Y}\widehat{Y}} \neq \emptyset$. This bad event occurs when $\exists i, j, l \in [q]$ with $i \neq j$ and $i \neq l$ such that $X^i = X^j$ and $\widehat{Y}^i = \widehat{Y}^l$. Let's first fix the values for the indices i, j and l. The probability of each of the events comes out to be at most $(2/N)$ due to the n-bit randomness of X^i or X^j and $\widehat{Y}^i$ or $\widehat{Y}^j$. As we can choose the index i in q ways and for each of those choices, we can choose each of the indices j and l in $(q-1)$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-13}] \leq \frac{q(q-1)^2}{N^2}\,. \tag{138}$$

– badμ-inner-14. $\mathcal{I}_{\widehat{Y}\widehat{Y}} \cap \mathcal{I}_{ZZ} \neq \emptyset$. This bad event occurs when $\exists i, j, l \in [q]$ with $i \neq j$ and $i \neq l$ such that $\widehat{Y}^i = \widehat{Y}^j$ and $Z^i = Z^l$. Let's first fix the values for the indices i, j and l. The probability of each of the events comes out to be at most $(2/N)$ due to the n-bit randomness of $\widehat{Y}^i$ or $\widehat{Y}^j$ and Z^i or Z^j. As we can choose the index i in q ways and for each of those choices, we can choose each of the indices j and l in $(q-1)$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-14}] \leq \frac{q(q-1)^2}{N^2}\,. \tag{139}$$

– badμ-inner-15. $\mathcal{I}_{ZZ} \cap \mathcal{I}_{XX} \neq \emptyset$. This bad event occurs when $\exists i, j, l \in [q]$ with $i \neq j$ and $i \neq l$ such that $Z^i = Z^j$ and $X^i = X^l$. Let's first fix the values for the indices i, j and l. The probability of each of the events comes out to be at most $(2/N)$ due to the n-bit randomness of Z^i or Z^j and X^i or X^j. As we can choose the index i in q ways and for each of those choices, we can choose each of the indices j and l in $(q-1)$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\mu\text{-inner-15}] \leq \frac{q(q-1)^2}{N^2}\,. \tag{140}$$

By combining Eqn. (126)-Eqn. (140), we have

$$\Pr[\text{bad}\mu\text{-inner}] \leq \frac{q(q_2q_3 + q_3q_4 + q_1q_4)}{N^2} + \frac{3q^2(q_2 + q_3 + q_4)}{N^2} + \frac{3q^3}{N^2}. \tag{141}$$

A.10 Bounding badμ-3coll

Proposition 10 *Having defined the bad event badμ-3coll in Fig. 7, we have*

$$\Pr[\textit{bad}\mu\textit{-3coll}] \le \frac{4\binom{q}{3}}{N^2}.$$

To prove the proposition, we first fix the values for the indices i, j and l.

- badμ-3coll-1. $i, j, l \in [q]$ with $i < j < l$ such that $X^i = X^j = X^l$. We can write $\Pr[X^i = X^j = X^l] = \Pr[X^i = X^j] \cdot \Pr[X^i = X^j = X^l | X^i = X^j]$ (as $\Pr[X^i = X^j = X^l | X^i \neq X^j] = 0$). Each term on the RHS can be at most $(2/N)$ due to the randomness over X^j and X^l respectively.
- badμ-3coll-2. $i, j, l \in [q]$ with $i < j < l$ such that $\widehat{Y}^i = \widehat{Y}^j = \widehat{Y}^l$. We can write $\Pr[\widehat{Y}^i = \widehat{Y}^j = \widehat{Y}^l] = \Pr[\widehat{Y}^i = \widehat{Y}^j] \cdot \Pr[\widehat{Y}^i = \widehat{Y}^j = \widehat{Y}^l | \widehat{Y}^i = \widehat{Y}^j]$ (as $\Pr[\widehat{Y}^i = \widehat{Y}^j = \widehat{Y}^l | \widehat{Y}^i \neq \widehat{Y}^j] = 0$). Each term on the RHS can be at most $(2/N)$ due to the randomness over $\widehat{Y}^j$ and $\widehat{Y}^l$ respectively.
- badμ-3coll-3. $i, j, l \in [q]$ with $i < j < l$ such that $Z^i = Z^j = Z^l$. We can write $\Pr[Z^i = Z^j = Z^l] = \Pr[Z^i = Z^j] \cdot \Pr[Z^i = Z^j = Z^l | Z^i = Z^j]$ (as $\Pr[Z^i = Z^j = Z^l | Z^i \neq Z^j] = 0$). Each term on the RHS can be at most $(2/N)$ due to the randomness over Z^j and Z^l respectively.

As we can choose the 3-tuple of indices (i, j, l) in $\binom{q}{3}$ ways, we use the union bound over all those possible choices to obtain

$$\Pr[\mathsf{bad}\mu\text{-}\mathsf{3col}] \le \frac{4\binom{q}{3}}{N^2}. \tag{142}$$

A.11 Bounding badμ-size

Proposition 11 *Having defined the bad event badμ-size in Fig. 7, we have*

$$\Pr[\textit{bad}\mu\textit{-size}] \le \frac{q^{1/2}(q_2 + q_3 + q_4)}{N} + \frac{2q^{3/2}}{N}.$$

We say that the bad event badμ-size happens if one of the following event happens.

- badμ-size-prim This event holds if either of the following three events hold:
  - badμ-size-$\mathcal{I}_X$: This event holds if $|\mathcal{I}_X| > q^{1/2}$.
  - badμ-size-$\mathcal{I}_{\widehat{Y}}$: This event holds if $|\mathcal{I}_{\widehat{Y}}| > q^{1/2}$.
  - badμ-size-$\mathcal{I}_Z$: This event holds if $|\mathcal{I}_Z| > q^{1/2}$.
- badμ-size-coll This event holds if either of the following three events hold:
  - badμ-size-$\mathcal{I}_{XX}$: This event holds if $|\mathcal{I}_{XX}| > q^{1/2}$.
  - badμ-size-$\mathcal{I}_{\widehat{Y}\widehat{Y}}$: This event holds if $|\mathcal{I}_{\widehat{Y}\widehat{Y}}| > q^{1/2}$.
  - badμ-size-$\mathcal{I}_{ZZ}$: This event holds if $|\mathcal{I}_{ZZ}| > q^{1/2}$.

A.11.1 Bounding badμ-size-prim

To bound this event, we bound each of the following events: badμ-size-$\mathcal{I}_X$, badμ-size-$\mathcal{I}_{\widehat{Y}}$, and bad$\mu$-size-$\mathcal{I}_Z$. We begin with bounding the size of $|\mathcal{I}_X|$. Let for each $i \in [q]$, $\mathbb{I}_i$ be an indicator random variable that takes the value 1 if there exists an $j \in [q_2]$ such that $X^i + K_2 = U_2^j$. Note that, the probability of this event holds is at most q_2/N using the randomness of key K_2, i.e., for a fixed $i \in [q]$,

$$\Pr[\mathbb{I}_i = 1] \le \frac{q_2}{N}.$$

Therefore, by the linearity of expectations and by applying Markov's inequality, we have

$$\Pr[|\mathcal{I}_X| > q^{1/2}] \leq \frac{q^{1/2}q_2}{N} \approx \frac{q^{3/2}}{N}, \qquad \text{(provided, } q_2 \approx q\text{)}.$$

In a similar way, we can show that

$$\Pr[|\mathcal{I}_{\widehat{Y}}| > q^{1/2}] \leq \frac{q^{1/2}q_3}{N}, \quad \Pr[|\mathcal{I}_Z| > q^{1/2}] \leq \frac{q^{1/2}q_4}{N}.$$

By combining the above three cases, we have

$$\Pr[\mathsf{bad}\mu\text{-}\mathsf{size}\text{-}\mathsf{prim}] \leq \frac{q^{1/2}(q_2+q_3+q_4)}{N}. \tag{143}$$

A.11.2 Bounding badμ-size-coll

To bound this event, we bound each of the following events: badμ-size-$\mathcal{I}_{XX}$, badμ-size-$\mathcal{I}_{\widehat{Y}\widehat{Y}}$, and bad$\mu$-size-$\mathcal{I}_{ZZ}$. We begin with bounding the size of $|\mathcal{I}_{XX}|$. Let for each $i \in [q]$, $\mathbb{I}_i$ be an indicator random variable that takes the value 1 if there exists an $j \in [q]$ with $j \neq i$ such that $X^i = X^j$. Note that, the probability of this event holds is at most q/N using the randomness of key $\widehat{R}^i$ (as $i \notin \mathcal{I}_R$), i.e., for a fixed $i \in [q]$,

$$\Pr[\mathbb{I}_i = 1] \leq \frac{q}{N}.$$

Therefore, by the linearity of expectations and by applying Markov's inequality, we have

$$\Pr[|\mathcal{I}_{XX}| > q^{1/2}] \leq \frac{q^{3/2}}{2N}.$$

In a similar way, we can show that

$$\Pr[|\mathcal{I}_{\widehat{Y}\widehat{Y}}| > q^{1/2}] \leq \frac{q^{3/2}}{2N}, \quad \Pr[|\mathcal{I}_{ZZ}| > q^{1/2}] \leq \frac{q^{3/2}}{2N}.$$

By combining the above three cases, we have

$$\Pr[\mathsf{bad}\mu\text{-}\mathsf{size}\text{-}\mathsf{coll}] \leq \frac{2q^{3/2}}{N}. \tag{144}$$

Finally, by combining Eqn. (143) and Eqn. (144), we have

$$\Pr[\mathsf{bad}\mu\text{-}\mathsf{size}] \leq \frac{q^{1/2}(q_2+q_3+q_4)}{N} + \frac{2q^{3/2}}{N}.$$

A.12 Bounding badλ-prim

Proposition 12 *Having defined the bad event badλ-prim in Fig. 8, we have*

$$\Pr[\mathit{bad}\lambda\text{-}\mathit{prim}] \leq \frac{qq_2(q_1+q_3+q_4+q_5)}{N^2} + \frac{qq_3(q_1+q_2+q_4+q_5)}{N^2} + \frac{qq_4(q_1+q_2+q_3+q_5)}{N^2} + \frac{7q^2(q_2+q_3+q_4)}{N^2}.$$

We say that the bad event badλ-prim happens if one of the following event happens.

- badλ-prim 1. $\exists i \in (\mathcal{I}_X \sqcup \mathcal{I}_{**})^c$ and $j \in [q_2]$ such that $\widehat{X}^i + k_2 = V_2^j$.
- badλ-prim 2. $\exists i \in (\mathcal{I}_{\widehat{Y}} \sqcup \mathcal{I}_{**})^c$ and $j \in [q_3]$ such that $Y^i + k_3 = V_3^j$.
- badλ-prim 3. $\exists i \in (\mathcal{I}_Z \sqcup \mathcal{I}_{**})^c$ and $j \in [q_4]$ such that $\widehat{Z}^i + k_4 = V_4^j$.

In the following subsections, we bound the above events.

A.12.1 Bounding badλ-prim 1

To bound this event, we further split it into various sub-cases and bound their individual probabilities as follows:

- badλ-prim 1a. $\exists i \in \mathcal{I}_R$ and $j \in [q_2]$ such that $\widehat{X}^i + K_2 = V_2^j$. In other words, $\exists i \in [q]$, $j \in [q_2]$ and $l \in [q_1]$ such that $R^i + K_1 = U_1^l$ and $\widehat{X}^i + K_2 = V_2^j$. Let's first fix the values for the indices i, j and l. The probability of each of the events $R^i + K_1 = U_1^l$ and $\widehat{X}^i + K_2 = V_2^j$ comes out to be $1/N^2$ each due to the randomness of the keys K_1 and K_2 respectively. As we can choose the index i, j and l in q, q_2 and q_1 ways respectively, we use the union bound over all those possible choices to obtain
$$\Pr[\text{bad}\lambda\text{-prim } 1a] \leq \frac{q q_1 q_2}{N^2}\,. \tag{145}$$
- badλ-prim 1b. $\exists i \in \mathcal{I}_S$ and $j \in [q_2]$ such that $\widehat{X}^i + K_2 = V_2^j$. Analysis of this bad event is similar to that of badλ-prim 1a, where we use the randomness of K_5 and K_2. Looking ahead, we bound the probability of the event to at most
$$\Pr[\text{bad}\lambda\text{-prim } 1b] \leq \frac{q q_2 q_5}{N^2}\,. \tag{146}$$
- badλ-prim 1c. $\exists i \in \mathcal{I}_{RR}$ and $j \in [q_2]$ such that $\widehat{X}^i + K_2 = V_2^j$. Analysis of this bad event is similar to that of badλ-prim 1a, where we use the randomness of R^i and K_2. Looking ahead, we bound the probability of the event to at most
$$\Pr[\text{bad}\lambda\text{-prim } 1c] \leq \frac{q^2 q_2}{2N^2}\,. \tag{147}$$
- badλ-prim 1d. $\exists i \in \mathcal{I}_{SS}$ and $j \in [q_2]$ such that $\widehat{X}^i + K_2 = V_2^j$. Again, analysis of this bad event is similar to that of badλ-prim 1c, where we use the randomness of S^i and K_2. Looking ahead, we bound the probability of the event to at most
$$\Pr[\text{bad}\lambda\text{-prim } 1d] \leq \frac{q^2 q_2}{2N^2}\,. \tag{148}$$
- badλ-prim 1e. $\exists i \in \mathcal{I}_{\widehat{Y}}$ and $j \in [q_2]$ such that $\widehat{X}^i + K_2 = V_2^j$. In other words, $\exists i \in [q]$, $j \in [q_2]$ and $l \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^l$ and $\widehat{X}^i + K_2 = V_2^j$. Let's first fix the values for the indices i, j and l. The probability of each of the events $\widehat{Y}^i + K_3 = V_3^l$ and $\widehat{X}^i + K_2 = V_2^j$ comes out to be $1/N^2$ due to the randomness of the keys K_2 and K_3. As we can choose the index i, j and l in q, q_2 and q_3 ways , we use the union bound over all those possible choices to obtain
$$\Pr[\text{bad}\lambda\text{-prim } 1e] \leq \frac{q q_2 q_3}{N^2}\,. \tag{149}$$
- badλ-prim 1f. $\exists i \in \mathcal{I}_Z$ and $j \in [q_2]$ such that $\widehat{X}^i + K_2 = V_2^j$. Analysis of this bad event is similar to that of badλ-prim 1e, where we use the randomness of K_4 and K_2. Looking ahead, we bound the probability of the above event to at most
$$\Pr[\text{bad}\lambda\text{-prim } 1f] \leq \frac{q q_2 q_4}{N^2}\,. \tag{150}$$
- badλ-prim 1g. $\exists i \in \mathcal{I}_{XX}$ and $j \in [q_2]$ such that $\widehat{X}^i + K_2 = V_2^j$. In other words, $\exists i \in [q]$, $j \in [q_2]$ and $l \in [q]$ such that $i \neq l$ and $X^i = X^l, \widehat{X}^i + K_2 = V_2^j$, which we equivalently write as
$$\widehat{R}^i + \widehat{R}^l = L^i + L^l, \widehat{X}^i + K_2 = V_2^j.$$
For a fixed choice of indices, we use the randomness of $\widehat{R}^i$ and K_2 to bound the probability of the event to at most $2/N^2$. As we can choose the index i, j and l in q, q_2 and $(q-1)$ ways respectively, we use the union bound over all those possible choices to obtain
$$\Pr[\text{bad}\lambda\text{-prim } 1g] \leq \frac{2q^2 q_2}{N^2}\,. \tag{151}$$

– badλ-prim $1h$. $\exists i \in \mathcal{I}_{\widehat{Y}\widehat{Y}}$ and $j \in [q_2]$ such that $\widehat{X}^i + K_2 = V_2^j$. In other words, $\exists i \in [q]$, $j \in [q_2]$ and $l \in [q]$ such that $i \neq l$ and $\widehat{Y}^i = \widehat{Y}^l, \widehat{X}^i + K_2 = V_2^j$, which we equivalently write as

$$\widehat{R}^i + \widehat{R}^l + \widehat{S}^i + \widehat{S}^l = L^i + T^i + L^l + T^l, \widehat{X}^i + K_2 = V_2^j.$$

For a fixed choice of indices, we use the randomness of $\widehat{R}^i$ and K_2 to bound the probability of the event to at most $2/N^2$. As we can choose the index i, j and l in q, q_2 and $(q-1)$ ways respectively, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\lambda\text{-prim } 1h] \leq \frac{2q^2 q_2}{N^2}\,. \tag{152}$$

– badλ-prim $1i$. $\exists i \in \mathcal{I}_{ZZ}$ and $j \in [q_2]$ such that $\widehat{X}^i + k_2 = V_2^j$. In other words, $\exists i \in [q]$, $j \in [q_2]$ and $l \in [q]$ such that $i \neq l$ and $Z^i = Z^l, \widehat{X}^i + K_2 = V_2^j$, which we equivalently write as

$$\widehat{S}^i + \widehat{S}^l = T^i + T^l, \widehat{X}^i + K_2 = V_2^j.$$

For a fixed choice of indices, we use the randomness of $\widehat{S}^i$ and K_2 to bound the probability of the event to at most $2/N^2$. As we can choose the index i, j and l in q, q_2 and $(q-1)$ ways respectively, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\lambda\text{-prim } 1i] \leq \frac{2q^2 q_2}{N^2}\,. \tag{153}$$

Adding all the above nine cases, we obtain

$$\Pr[\text{bad}\lambda\text{-prim } 1] \leq \frac{q q_2 (q_1 + q_3 + q_4 + q_5 + 7q)}{N^2}\,. \tag{154}$$

A.12.2 Bounding badλ-prim 2.

As before, to bound this event, we further split it into various sub-cases and bound their individual probabilities as follows:

– badλ-prim $2a$. $\exists i \in \mathcal{I}_R$ and $j \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^j$. In other words, $\exists i \in [q]$, $j \in [q_2]$ and $l \in [q_1]$ such that $R^i + K_1 = U_1^l$ and $\widehat{Y}^i + K_3 = V_3^j$. Let's first fix the values for the indices i, j and l. The probability of each of the events $R^i + K_1 = U_1^l$ and $\widehat{Y}^i + K_3 = V_3^j$ comes out to be $1/N^2$ each due to the randomness of the keys K_1 and K_3 respectively. As we can choose the index i, j and l in q, q_3 and q_1 ways respectively, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\lambda\text{-prim } 2a] \leq \frac{q q_1 q_3}{N^2}\,. \tag{155}$$

– badλ-prim $2b$. $\exists i \in \mathcal{I}_S$ and $j \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^j$. Analysis of this bad event is similar to that of badλ-prim $2a$, where we use the randomness of K_5 and K_3. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 2b] \leq \frac{q q_3 q_5}{N^2}\,. \tag{156}$$

– badλ-prim $2c$. $\exists i \in \mathcal{I}_{RR}$ and $j \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^j$. Analysis of this bad event is similar to that of badλ-prim $2a$, where we use the randomness of R^i and K_3. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 2c] \leq \frac{q^2 q_3}{2N^2}\,. \tag{157}$$

– badλ-prim 2d. $\exists i \in \mathcal{I}_{SS}$ and $j \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^j$. Analysis of this bad event is similar to that of badλ-prim 2c, where we use the randomness of S^i and K_3. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 2d] \le \frac{q^2 q_3}{2N^2}\,. \tag{158}$$

– badλ-prim 2e. $\exists i \in \mathcal{I}_Z$ and $j \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^j$. Analysis of this bad event is again similar to that of badλ-prim 1f, where we use the randomness of K_4 and K_3. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 2e] \le \frac{q q_3 q_4}{N^2}\,. \tag{159}$$

– badλ-prim 2f. $\exists i \in \mathcal{I}_X$ and $j \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^j$. Analysis of this bad event is again similar to that of badλ-prim 2a, where we use the randomness of K_2 and K_3. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 2f] \le \frac{q q_2 q_3}{N^2}\,. \tag{160}$$

– badλ-prim 2g. $\exists i \in \mathcal{I}_{XX}$ and $j \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^j$. Analysis of this event is similar to that of badλ-prim 1g, where we use the randomness of $\widehat{R}^i$ and K_3. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 2g] \le \frac{2q^2 q_3}{N^2}\,. \tag{161}$$

– badλ-prim 2h. $\exists i \in \mathcal{I}_{\widehat{Y}\widehat{Y}}$ and $j \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^j$. Analysis of this event is similar to that of badλ-prim 1h, where we use the randomness of $\widehat{R}^i$ and K_3. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 2h] \le \frac{2q^2 q_3}{N^2}\,. \tag{162}$$

– badλ-prim 2i. $\exists i \in \mathcal{I}_{ZZ}$ and $j \in [q_3]$ such that $\widehat{Y}^i + K_3 = V_3^j$. Again, the analysis of this event is similar to that of badλ-prim 1i, where we use the randomness of $\widehat{S}^i$ and K_3. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 2i] \le \frac{2q^2 q_3}{N^2}\,. \tag{163}$$

Adding all the above nine cases, we obtain

$$\Pr[\text{bad}\lambda\text{-prim } 2] \le \frac{q q_3 (q_1 + q_2 + q_4 + q_5 + 7q)}{N^2}\,. \tag{164}$$

A.12.3 Bounding badλ-prim 3.

As before, to bound this event, we further split it into various sub-cases and bound their individual probabilities as follows:

– badλ-prim 3a. $\exists i \in \mathcal{I}_R$ and $j \in [q_4]$ such that $\widehat{Z}^i + K_4 = V_4^j$. In other words, $\exists i \in [q]$, $j \in [q_4]$ and $l \in [q_1]$ such that $R^i + K_1 = U_1^l$ and $\widehat{Z}^i + K_4 = V_4^j$. Let's first fix the values for the indices i, j and l. The probability of each of the events $R^i + K_1 = U_1^l$ and $\widehat{Z}^i + K_4 = V_4^j$ comes out to be $1/N^2$ each due to the randomness of the keys K_1 and K_4 respectively. As we can choose the index i, j and l in q, q_4 and q_1 ways respectively, we use the union bound over all those possible choices to obtain

$$\Pr[\text{bad}\lambda\text{-prim } 3a] \le \frac{q q_1 q_4}{N^2}\,. \tag{165}$$

- badλ-prim 3b. $\exists i \in \mathcal{I}_S$ and $j \in [q_4]$ such that $\widehat{Z}^i + K_4 = V_4^j$. Analysis of this bad event is similar to that of badλ-prim 3a, where we use the randomness of K_5 and K_4. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 3b] \le \frac{qq_4q_5}{N^2}\,. \tag{166}$$

- badλ-prim 3c. $\exists i \in \mathcal{I}_{RR}$ and $j \in [q_4]$ such that $\widehat{Z}^i + K_4 = V_4^j$. Analysis of this bad event is similar to that of badλ-prim 3a, where we use the randomness of R^i and K_4. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 3c] \le \frac{q^2q_4}{2N^2}\,. \tag{167}$$

- badλ-prim 3d. $\exists i \in \mathcal{I}_{SS}$ and $j \in [q_4]$ such that $\widehat{Z}^i + K_4 = V_4^j$. Analysis of this bad event is similar to that of badλ-prim 3a, where we use the randomness of S^i and K_4. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 3d] \le \frac{q^2q_4}{2N^2}\,. \tag{168}$$

- badλ-prim 3e. $\exists i \in \mathcal{I}_X$ and $j \in [q_4]$ such that $\widehat{Z}^i + K_4 = V_4^j$. Analysis of this bad event is similar to that of badλ-prim 3a, where we use the randomness of K_2 and K_4. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 3e] \le \frac{qq_2q_4}{N^2}\,. \tag{169}$$

- badλ-prim 3f. $\exists i \in \mathcal{I}_{\widehat{Y}}$ and $j \in [q_4]$ such that $\widehat{Z}^i + K_4 = V_4^j$. Analysis of this bad event is similar to that of badλ-prim 3a, where we use the randomness of K_3 and K_4. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 3f] \le \frac{qq_3q_4}{N^2}\,. \tag{170}$$

- badλ-prim 3g. $\exists i \in \mathcal{I}_{XX}$ and $j \in [q_4]$ such that $\widehat{Z}^i + K_4 = V_4^j$. Analysis of this bad event is similar to that of badλ-prim 1g, where we use the randomness of $\widehat{R}^i$ and K_4. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 3g] \le \frac{2q^2q_4}{N^2}\,. \tag{171}$$

- badλ-prim 3h. $\exists i \in \mathcal{I}_{\widehat{Y}\widehat{Y}}$ and $j \in [q_4]$ such that $\widehat{Z}^i + K_4 = V_4^j$. Analysis of this bad event is similar to that of badλ-prim 1h, where we use the randomness of $\widehat{R}^i$ and K_4. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 3h] \le \frac{2q^2q_4}{N^2}\,. \tag{172}$$

- badλ-prim 3i. $\exists i \in \mathcal{I}_{ZZ}$ and $j \in [q_4]$ such that $\widehat{Z}^i + K_4 = V_4^j$. Analysis of this bad event is similar to that of badλ-prim 1i, where we use the randomness of $\widehat{S}^i$ and K_4. Looking ahead, we bound the probability of the event to at most

$$\Pr[\text{bad}\lambda\text{-prim } 3i] \le \frac{2q^2q_4}{N^2}\,. \tag{173}$$

Adding all the above nine cases, we obtain

$$\Pr[\text{bad}\lambda\text{-prim } 3] \le \frac{qq_4(q_1 + q_2 + q_3 + q_5 + 7q)}{N^2}\,. \tag{174}$$

A.13 Bounding badλ-coll

Proposition 13 *Having defined the bad event badλ-coll in Fig. 8, we have*

$$\Pr[\textit{bad}\lambda\textit{-coll}] \le \frac{\binom{q}{2}(5q + q_1 + q_2 + q_3 + q_4 + q_5)}{N^2}.$$

We say that the bad event badλ-coll happens, if one of the following event happens.

- badλ-coll 1. $\exists i \in \mathcal{I}^c_{**}, j \in [q]$ and $i \neq j$ such that $X^i \neq X^j$ and $\widehat{X}^i = \widehat{X}^j$.
- badλ-coll 2. $\exists i \in \mathcal{I}^c_{**}, j \in [q]$ and $i \neq j$ such that $\widehat{Y}^i \neq \widehat{Y}^j$ and $Y^i = Y^j$.
- badλ-coll 3. $\exists i \in \mathcal{I}^c_{**}, j \in [q]$ and $i \neq j$ such that $Z^i \neq Z^j$ and $\widehat{Z}^i = \widehat{Z}^j$.

In the following subsection, we bound the above events. To do this, we first define a condition set and then analyze these three bad events on that condition set.

Condition Set

1. $\exists i \in \mathcal{I}_R$. In other words, $\exists i \in [q]$ and $k \in [q_1]$ such that $R^i + K_1 = U^k_1$.
2. $\exists i \in \mathcal{I}_S$. In other words, $\exists i \in [q]$ and $k \in [q_5]$ such that $S^i + K_5 = U^k_5$.
3. $\exists i \in \mathcal{I}_{RR}$. In other words, $\exists i \in \mathcal{I}_{\mathsf{dec}}$ and $k \in [i-1]$ such that $R^i = R^k$.
4. $\exists i \in \mathcal{I}_{SS}$. In other words, $\exists i \in \mathcal{I}_{\mathsf{enc}}$ and $k \in [i-1]$ such that $S^i = S^k$.
5. $\exists i \in \mathcal{I}_X$. In other words, $\exists i \in [q]$ and $k \in [q_2]$ such that $X^i + K_2 = U^k_2$.
6. $\exists i \in \mathcal{I}_{\widehat{Y}}$. In other words, $\exists i \in [q]$ and $k \in [q_3]$ such that $\widehat{Y}^i + K_3 = U^k_3$.
7. $\exists i \in \mathcal{I}_Z$. In other words, $\exists i \in [q]$ and $k \in [q_4]$ such that $Z^i + K_4 = U^k_4$.
8. $\exists i \in \mathcal{I}_{XX}$. In other words, $\exists i, k \in [q]$ with $i \neq j$ such that $X^i = X^k$.
9. $\exists i \in \mathcal{I}_{\widehat{Y}\widehat{Y}}$. In other words, $\exists i, k \in [q]$ with $i \neq j$ such that $\widehat{Y}^i = \widehat{Y}^k$.
10. $\exists i \in \mathcal{I}_{ZZ}$. In other words, $\exists i, k \in [q]$ with $i \neq j$ such that $Z^i = Z^k$.

Let's first fix the values for the indices i, j and k. For any of badλ-coll 1, badλ-coll 2 and badλ-coll 3, any one of the conditions from the above condition set satisfies. Once we fix that condition, the probability of that condition comes out to be $(1/N)$. On the other hand, the probability of the event $\widehat{X}^i = \widehat{X}^j$ is at most $(2/N)$ when $j \in \mathcal{I}_X$, and is equal to $(1/N)$ otherwise. Similarly, the probability of the event $Y^i = Y^j$ is at most $(2/N)$ when $j \in \mathcal{I}_Y$, and is equal to $(1/N)$ otherwise; and the probability of the event $\widehat{Z}^i = \widehat{Z}^j$ is at most $(2/N)$ when $j \in \mathcal{I}_Z$, and is equal to $(1/N)$ otherwise. Now one can choose the pair of indices (i, j) in $\binom{q}{2}$ ways, and the index k in as many ways as the maximum number of queries to the relevant permutation (in case of condition 1, 2, 5, 6 and 7) or in q ways (otherwise). Using the union bound over all those possible indices, we obtain the upper bound of each of these bad events as $(2q \cdot \binom{q}{2})/(N^2)$ or $(2q_l \cdot \binom{q}{2})/(N^2)$ (where the relevant permutation is P_l).