1 $m = kn$

1.1 6-rounds

We proved 6-round expanding feistel construction which can achieve CCA security under related-key attacks with the simple key assignments:$[1, 2, 1, 2, 1, 2]$.

$$\frac{\Pr_{re}(\tau)}{Pr_{id}(\tau)} \geq 1 - (\frac{9q^2}{2^n} + \frac{q^2}{2^{3n}}) \tag{1}$$

Proof: To prove Eq.(1),we distinguish good and bad key with respect to τ, and finally analyze the probability of the good key to get the advantage of this construction.
First, we classify ϕ_i, suppose that the quantity of $\phi^{(i)}$ is α.
$\mathcal{Q}_1 = (\phi^{(1)}, X_{11}[1, 4n], X_{71}[1, 4n]), \ldots, (\phi^{(1)}, X_{1q_1}[1, 4n], X_{7q_1}[1, 4n])$ which has q_1 different input totally.
$\mathcal{Q}_2 = (\phi^{(2)}, X_{12}[1, 3n], X_{72}[1, 4n]), \ldots, (\phi^{(2)}, X_{1q_2}[1, 4n], X_{7q_2}[1, 4n])$ which has q_2 different input totally.
$\vdots$
$\mathcal{Q}_\alpha = (\phi^{(\alpha)}, X_{1\alpha}[1, 4n], X_{7\alpha}[1, 4n]), \ldots, (\phi^{(\alpha)}, X_{1q_\alpha}[1, 4n], X_{7q_\alpha}[1, 4n])$ which has q_α different input totally.
Suppose that there are α $\phi^{(i)}$ which can derive β different $\mathcal{K}_1$: $\mathcal{K}_1^{(1)}$, $\mathcal{K}_1^{(2)}$, $\ldots$,$\mathcal{K}_1^{(\beta)}(\beta \leq \alpha)$.
Suppose that q Related-Key Oracle query constitute of $q_1^* \ldots q_\beta^*$ inputs separately in β different $\mathcal{K}_1$.
Bad Keys are now defined as follows.
Definition 1: $\mathcal{K}_1^{bad}$ for 6 Rounds with respect to τ, $\mathcal{K}_1$ is *bad*, if the following conditions is fulfilled
(B-1)there exists i and j such that $X_{4,i}[1, n] = X_{4,j}[1, n], (i \neq j)$
(B-2)there exists i and j such that $X_{4,i}[1, n] = X_{2,j}[1, n]$
(B-3)there exists i and j such that $X_{4,i}[1, n] = X_{6,j}[1, n]$
Otherwise we say $\mathcal{K}_1$ is *good*.
Definition 2: $\mathcal{K}_2^{bad}$ for 6 Rounds with respect to τ, $\mathcal{K}_2$ is *bad*, if the following conditions is fulfilled
(B-1)there exists i and j such that $X_{3,i}[1, n] = X_{3,j}[1, n], (i \neq j)$
(B-2)there exists i and j such that $X_{3,i}[1, n] = X_{1,j}[1, n]$
(B-3)there exists i and j such that $X_{3,i}[1, n] = X_{5,j}[1, n]$
(B-4)there exists i and j such that $X_{3,i}[1, n] = X_{2,j}[1, n]$
(B-5)there exists i and j such that $X_{3,i}[1, n] = X_{4,j}[1, n]$
(B-6)there exists i and j such that $X_{3,i}[1, n] = X_{6,j}[1, n]$
Otherwise we say $\mathcal{K}_2$ is *good*.
For $\mathcal{K}_1^{bad}$,we can get the probability:
$\Pr[\mathcal{K}_1^{bad}] \leq (\frac{3}{2^n})q^2$
For $\mathcal{K}_2^{bad}$,we can get the probability:
$\Pr[\mathcal{K}_2^{bad}] \leq (\frac{6}{2^n})q^2$
Lowering Bounding the Probability for Good Keys

We now lower bound the probability for good keys.
$\Pr_{re}[\tau] = (1 - \Pr[\mathcal{K}_1^{bad}])(\frac{1}{2^n})^{3q} \times (1 - \Pr[\mathcal{K}_2^{bad}])$

$$\begin{aligned}
\frac{\Pr_{re}(\tau)}{\Pr_{id}(\tau)} &= (1 - \Pr[\mathcal{K}_1^{bad}]) \times (\frac{1}{2^n})^q \times (1 - \frac{1}{2^{2n}})^q \times (1 - \Pr[\mathcal{K}_2^{bad}]) / \prod_{i=0}^{\alpha} \frac{1}{(2^{3n})_{q_i}} \\
&\geq (1 - \frac{3q^2}{2^n}) \times (1 - \frac{6q^2}{2^n}) \times (\frac{1}{2^n})^{3q} \times (2^{3n} - q)^q \\
&\geq (1 - \frac{9q^2}{2^n})(1 - \frac{q^2}{2^{3n}}) \\
&\geq 1 - (\frac{9q^2}{2^n} + \frac{q^2}{2^{3n}})
\end{aligned}$$

So if $q \ll 2^{\frac{n}{2}}$,we can get this construction is CCA-security.