表 4.9 S盒由 8 张数据表组成

| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | | | | | | | | | | | | (| | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----|----|----|----|----|----|----|----|-----|----|----|----|----|----|----|
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | S ₁ | | | | | | | | | | | | | | | |
| $\begin{array}{c c ccccccccccccccccccccccccccccccccc$ | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| $\begin{array}{c c c c c c c c c c c c c c c c c c c $ | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| $\begin{array}{c c c c c c c c c c c c c c c c c c c $ | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11_ | 3 | 14 | 10 | 0 | 6 | 13 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | S ₂ | | | | | | | | | | | | | | | |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| $\begin{array}{c c ccccccccccccccccccccccccccccccccc$ | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| $\begin{array}{c c ccccccccccccccccccccccccccccccccc$ | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | s_3 | | | | | | | | | | | | | | | |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| $\begin{array}{c c ccccccccccccccccccccccccccccccccc$ | 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | | | | | | | | S | 4 | | | | | | | |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| $\begin{array}{c c ccccccccccccccccccccccccccccccccc$ | 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9 14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6 4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14 11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3 8 12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11 10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8 9 14 15 5 2 8 12 3 7 0 4 10 1 13 </td <td>3</td> <td>15</td> <td>0</td> <td>6</td> <td>10</td> <td>1</td> <td>13</td> <td>8</td> <td>9</td> <td>4</td> <td>5</td> <td>11</td> <td>12</td> <td>7</td> <td>2</td> <td>14</td> | 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |
| 14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6 4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14 11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3 S6 12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11 10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6 | | | | | | | | S | 5 | | | | | | | |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| $\begin{array}{c ccccccccccccccccccccccccccccccccccc$ | 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11 10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6 | 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |
| 10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6 | | | | | | | | | | | | | | | | |
| 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6 | 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| | 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13 | 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| | 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | -0 | 8 | 13 |

| | S ₇ | | | | | | | | | | | | | | |
|----|----------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |
| | s_8 | | | | | | | | | | | | | | |
| 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |