Comparison Table:

| **Aspect** | **Original Logic** | **Proposed Logic** |
| --- | --- | --- |
| S-box Implementation | Two options: lookup table and optimized equations | Single set of simplified equations |
| S-box Complexity | More complex equations with multiple terms | Simpler equations using only XOR and AND operations |
| Round Constant Structure | Single always block for calculation and XOR | Separate calculation and XOR assignment |
| Round Constant Cases | If-else structure without default | Case structure with default |
| Counter Usage | Uses (ctr-1) | Uses ctr directly |
| 12-round Handling | Implicit (else condition) | Explicit case |

Key Points:

**Substitution layer**

1. S-box Simplification: Proposed logic significantly simplifies the S-box implementation, potentially leading to **more efficient hardware**, **using XOR and AND gates**
2. Uniform S-box Structure: Uses a **consistent pattern for all five S-box outputs**, which could **simplify understanding and implementation**.
3. Parallel Execution.

**Roundconstant**

1. Round Constant Modularity: Proposed round constant logic separates the **constant calculation from the XOR operation**, potentially improving readability and modularity.
2. Explicit Round Handling: logic explicitly handles all round cases, including 12 rounds, which may improve clarity and reduce potential errors.
3. Direct Counter Usage: By using the **counter directly instead of (ctr-1)**, your logic may simplify the hardware implementation slightly.

S-box optimized equations proposed by using the following logic

sl[i] = x[i] ^ (~x[(i+1)%5] & x[(i+2)%5])

//s-box proposed equations  
  
sl0 = x0 ^ (~x1 & x2);

sl1 = x1 ^ (~x2 & x3);

sl2 = x2 ^ (~x3 & x4);

sl3 = x3 ^ (~x4 & x0);

sl4 = x4 ^ (~x0 & x1);

This pattern identified a recurring relationship between the inputs and outputs of the S-box.

1. Analyzed the original S-box truth table or equations.
2. Observed patterns in how the outputs relate to the inputs.
3. Experimented with different Boolean expressions to find a simpler form that matches the S-box behavior.
4. Verified your simplified equations against the original S-box for all possible inputs.

For the round constant logic, proposed approach suggests:

1. Recognizing that the round constant only affects the least significant byte of the output.
2. Separating the constant calculation from the XOR operation for clarity.
3. Using a case statement to handle different round numbers more explicitly.
4. Adding a default case for robustness.