AES – 128

Introduction:

The Advanced Encryption Standard (AES) is a commonly used encryption technique that is critical for maintaining data security in modern systems. AES-128 is a variation of this technique that uses 128-bit data blocks and a 128-bit key. Because of its excellent cryptographic features and efficiency, AES-128 has been chosen by governments, organizations, and companies for the protection of sensitive data.
In this report, we will look at AES-128 and its hardware implementation as proposed by Homer Hsingutilising in "*AES Core Specification*" using Verilog. However, as the complexity of digital designs increases, more current languages, such as SystemVerilog, provide increased capabilities that make development and verification easier and more reliable. As a result, in this report will describe the Verilog to SystemVerilog conversion process to code enhancement.

What is AES-128?

The AES (Advanced Encryption Standard) is a symmetric encryption algorithm developed by the National Institute of Standards and Technology. AES encrypts data in blocks of 128 bits. AES-128 is one of three potential key lengths for AES (128, 192, and 256 bits) and is known for its security and performance.

Key steps in AES-128:

SubBytes is a non-linear substitution step that replaces each byte in the state with a value from a predefined substitution box (S-box). This replacement is done in such a way that a byte is never substituted by itself or by another byte that complements the current byte, increasing its resistance to attackers.

ShiftRows: The rows of the state matrix are shifted cyclically with varied offsets. This stage generates dispersion in encryption, which spreads the data over the matrix and reduces the predictability of byte placements.

MixColumns: This step involves multiplying a matrix. Every column is multiplied by a particular matrix, which modifies each byte's location within the column. (This step is skipped in the last round)

AddRoundKey: A round-specific key (derived from the original key) is added to the state via a bitwise XOR operation.

- The AES algorithm's AddRoundKey step uses several round keys to augment the 128-bit encryption key. This procedure guarantees that each cycle utilizes a unique key, which improves the encryption's security.
- AES-128 is made up of *ten rounds* of these processes, each of which increasingly encrypts the data.

Applied Differences from Verilog to SystemVerilog:

- The input and output ports are declared directly with their data types in the module header, making the code more compact and easier to understand.
- Combinational and sequential logic can both be implemented using the logic type, which simplifies coding and eliminates the possibility of confusing wire with reg.

```
reg [127:0] state;  →  logic [127:0] state;
wire [127:0] out;      logic [127:0] out;
```

- SystemVerilog introduces more specific always blocks for combinational and sequential logic, improving the clarity and functionality of the code.
  always_ff is used for sequential logic driven by flip-flops. (always replaced by always_ff where needed (not at the testbench)).
- Instead of manual checks (if statements) will use Built-in assert statements.

```
if (out !== 128'h3925841d02dc09fbdc118597196a0b32) begin
    $display("Error: Output mismatch");
    $finish;
End
```

↓

```
assert (out === 128'h3925841d02dc09fbdc118597196a0b32)
else begin

$fatal("Error: Output mismatch");

end
```

Results:

The testbench file is test_aes_128.sv for the AES-128. It will produce an error message if the output is incorrect. If not, the word "Good" is printed at the end.After the testing, the examined System Verilog method yielded the same outcome as the Verilog method, as shown in the following:

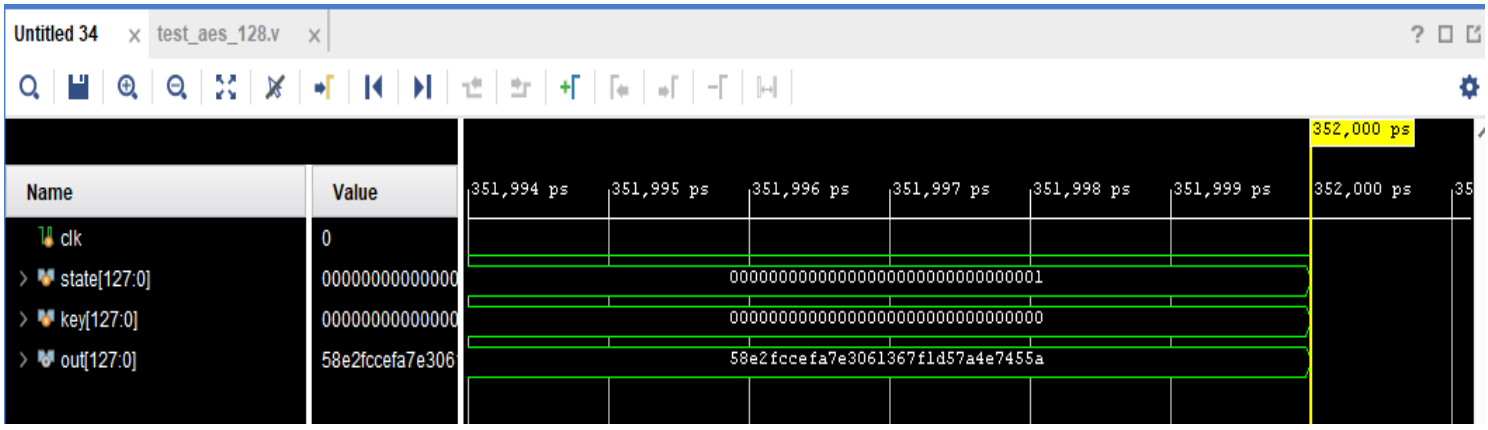

Figure 1 Expected output in Verilog

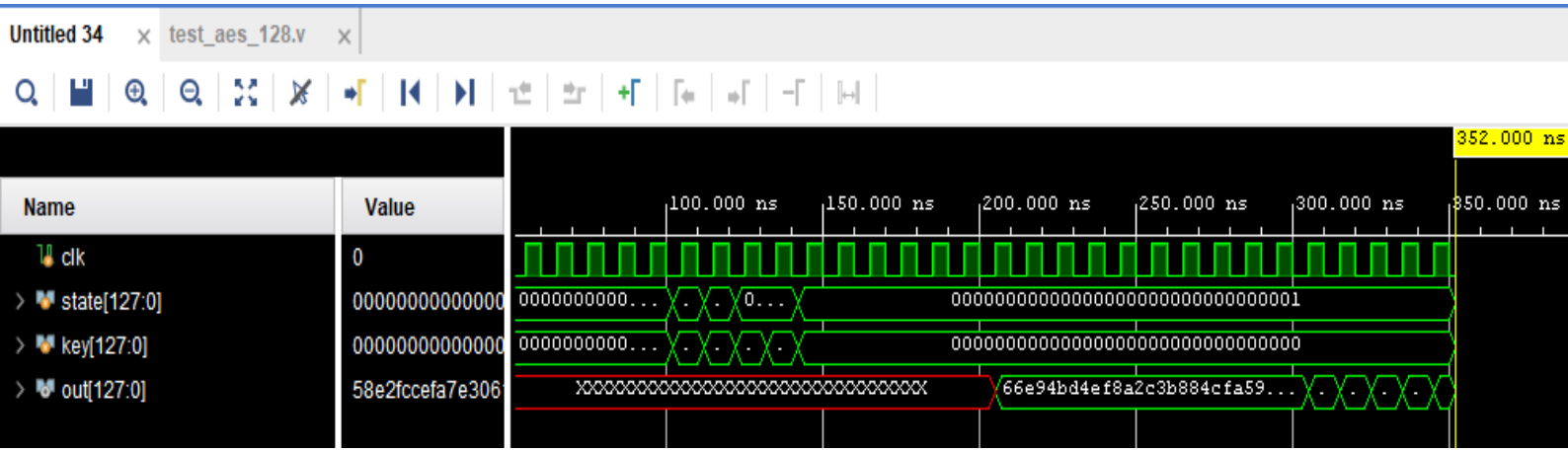

Figure 3 Behavioral simulation in Verilog

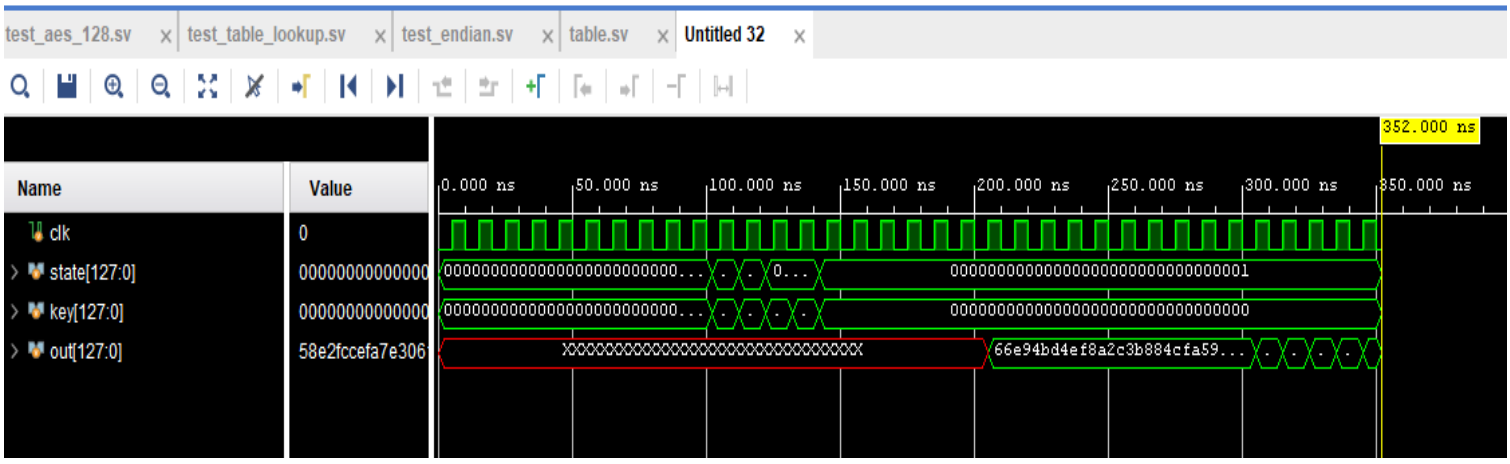

Figure 2 Behavioral simulation in System Verilog

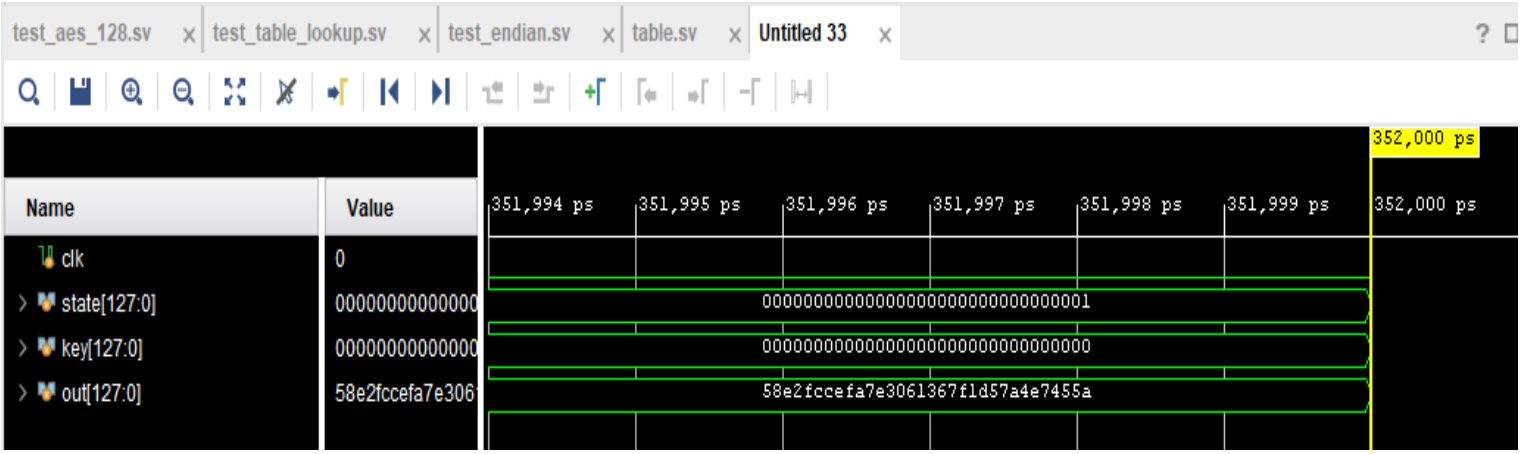

Figure 4 Expected output in System Verilog

References:

[1] Homer Hsing, AES Core Specification, 2013

[2] Advanced Encryption Standard- AES

https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

[3] Advanced Encryption Standard,

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard