WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Implementation of AES Algorithm using Verilog HDL

Reyna Varshini A, Saran S, Thamayanthi S

M.E VLSI Design and Embedded Systems, Department of Electronics Engineering, Madras Institute of Technology Campus, Anna University, Chennai, India

M.S.Vinotheni

Teaching Fellow, Department of Electronics Engineering, Madras Institute of Technology Campus, Anna University, Chennai, India

ABSTRACT:

Cryptography offers with the security and keenness of the information. At first numerous calculations were advanced to encode and translate the measurements in any case for securing colossal and secret data, the existing calculations are not solid, so AES turned into created as an unused favoured for scrambling and decoding records. At first, it is miles uncommonly utilized to ensure discernibly individual measurements, afterward numerous applications in organizing commenced the utilization of AES as a standard to ensure their data. It is customarily utilized to shield unstable records, in spite of the fact that it is additionally connected to community backends to enhance actualities security. AES utilizes pieces which can be 16 bytes long, and its keys can run in length from 128 bits to 256 bits. The major reason of the utilize of Verilog as restricted to common VHDL is that it manages exceptionally less operation time and the engendering delay to encode and translate the data are comparatively much less than distinctive HDL dialects. Sometime recently AES, DES changed into utilized as the encryption well known. The preeminent downside of DES is that the steady key length of fifty-six bits. This issue is illuminated by way of AES by means of giving the capacity of the utilize of required variable key length.

Introduction:

In the virtual age, statistics protection has become the main subject due to the exponential increase in online communication and information garage. While Cybermenaces keeps to develop, the call for powerful cryptographic techniques to guard touchy statistics from illegal access has end up more important than ever. Cryptography acts as a foundation for safe information transmission, protection, integrity, and authenticity. Among the distinctive cryptographic algorithms, the superior encryption fashionable (AES) is distinguished as one of the maximum symmetrical and reliable symmetrical encryption techniques.

Became standardized via the National Institute of Standards and Technology (NIST) in 2001, AES changed the antique records encoding widespread (of) and supplied a considerable development in protection and computer systems. AES works on fixed block sizes of 128 bits and helps the principle size of 128, 192 or 256 bits, which makes it able to adapting to exclusive safety requirements. The energy, velocity, and capacity to resist crypto attacks have installed it as a basis of current cryptographic structures. Therefore, AES is widely used in various programs, consisting of secure net verbal exchange, wireless network, included system, and cloud garage.

Recent advances within the crypto research have expanded AES applications similarly to imposing traditional software. In the sector of Internet of Things (IoT), AES Light's ideas had been developed to meet gadgets related to assets. Techniques which include pipeline structure, S packing containers are optimized and deployed ASIC / FPGA on the efficiency of improving energy even as retaining the potential to face up to aspect canal attacks consisting of special defect analysis (DFA). In addition, in the cloud surroundings, the introduction of dynamic AES locks, in conjunction with blockchain -based totally key management, presents improved security through preventing the primary compromise and allowing decentralized control mechanisms.
In addition, the combination of ISS with cryptographic techniques along with deep random bits (CTR DRBG), the code of the ellipse curve (ECC) and clever contracts has strengthened the principle exchange mechanism and records sharing. This procedure ensures a strong protection for secure conversation among systems. AES is likewise used with errors, allowing safety and dependable transmission in excessive environments. Its compatibility with hardware and software program systems makes it a super candidate for joint deployment, from mobile gadgets to excessive -performance servers.
In addition, continuous research on aspect canal assaults and financial performance principles may be reinforced than an extended -term cryptocurrency solution. With the growing requirements in complying with network safety and security rules, ISS's involvement keeps to develop the various fields of the Government, health care, finance, and industrial fields.

This article goals to find out the traits of the implementation and security of AES algorithm, highlighting its meaning in cutting-edge cryptographic systems. In addition, he'll study rising techniques to improve the performance and safety of AES, mainly in lighting fixtures structures, cloud computing

and real -time packages. By reading the latest manner and presenting optimized AES -based cryptography answers, this observe contributes to continuous development of secure and advanced encryption methods according with current digital threats.

Methodology:

The Advanced Encryption Standard (AES) is a symmetric-key cipher that operates iteratively and is primarily based on a substitution-permutation community, differing from the Feistel cipher structure employed in in advance encryption methods. It comprises a sequence of transformation rounds that put into effect both substitution and permutation processes to ensure information security. AES tactics records in byte-stage segments, mainly dealing with 128-bit blocks organized as a 4x4 matrix of sixteen bytes. This matrix is processed in a column-wise way and undergoes a couple of rounds of transformation. The overall wide variety of rounds is contingent upon the key length: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 1 round for 256-bit keys. Each round employs a wonderful 128-bit round key, derived through a process called key expansion from the authentic AES key

In a typical round of AES encryption, four key operations are performed:

1. Byte Substitution (SubBytes): Each byte in the 4x4 matrix is substituted with a corresponding value from a specific Substitution Box (S-box). This non-linear transformation introduces confusion, which is crucial for secure encryption.

2. ShiftRows: In this step, the rows of the matrix are cyclically shifted to the left. The first row remains unchanged. The second row is shifted one byte to the left. The third row shifts two bytes to the left. The fourth row moves three bytes to the left. This operation enhances inter-byte dependency by distributing the bytes across columns.

3. MixColumns: Each column of the matrix undergoes a linear transformation utilizing Galois Field arithmetic ($GF(2^8)$). This process amalgamates the four bytes within each column to produce new byte values, thereby enhancing the diffusion property of the cipher. It is important to note that this step is omitted in the final round.

4. AddRoundKey: The resultant 128-bit matrix is subjected to an XOR operation with the round key corresponding to the current round. This activity is repeated in each round with a separate circular touch created during the expansion of keys. In the final round, this step offered the final encryption text.

The AES decryption process mirrors the encryption procedure but executes the steps in reverse order, employing inverse transformations: Inverse AddRoundKey, Inverse MixColumns, Inverse ShiftRows, and Inverse SubBytes. Each decryption round reverses the modifications made during encryption. As AES does not utilize the Feistel structure, the encryption and decryption processes must be implemented separately, although they are closely related.

Overview of AES Algorithm Design

AES, additionally called Rijndael, became evolved by way of Belgian cryptographers Joan Daemen and Vincent Rijmen. It changed into decided on with the aid of the National Institute of Standards and Technology (NIST) in 2001 to update the old Data Encryption Standard (DES). AES is now the U.S. Government trendy for encrypting labelled statistics and is published as FIPS PUB 197. AES is a block cipher that strategies 128-bit blocks with key sizes of 128, 192, or 256 bits. Unlike DES, which employs a Feistel structure and a fifty-six-bit key, AES makes use of a substitution-permutation community that is green in each software and hardware implementations. The fashionable has been widely followed because of its robust security and high-speed overall performance. AES is also protected in the ISO/IEC 18033-three block cipher general and is the simplest publicly available cipher authorised by means of the NSA for top-secret records when utilized in authorised modules.

High-Level AES Algorithm Description

KeyExpansion: Round keys are generated from the original cipher key using a well-defined schedule. An additional key is generated for the initial AddRoundKey.

Initial Round:

AddRoundKey: XOR the plaintext with the first-round key.

Main Rounds (9, 11, or 13 times depending on key length):

SubBytes: Apply a non-linear substitution using the S-box.
ShiftRows: Perform row-wise cyclic shifts in the state matrix.
MixColumns: Apply a linear transformation to each column using fixed polynomial multiplication.
AddRoundKey: Combine the state with the current round key.

Final Round: SubBytes, ShiftRows, AddRoundKey.

Mathematical Basis for AES Transformations:
SubBytes: Substitution is performed via an S-box based on the multiplicative inverse in GF(2^8) combined with an affine transformation. The S-box is designed to avoid fixed points and enhance non-linearity.
ShiftRows: Byte positions in rows are cyclically shifted to prevent column independence and promote interdependency.
MixColumns: Each column is treated as a four-term polynomial and multiplied modulo $x^4 + 1$ with a fixed polynomial in GF(2^8). This ensures maximum diffusion and resistance to attacks.
AddRoundKey: A simple bitwise XOR between the current state and the round key, ensuring key-dependent transformations in each round.

Results:

The AES encryption module was developed utilizing Verilog HDL and synthesized through the Xilinx Vivado Design Suite. The implementation was specifically aimed at the Xilinx Artix-7 FPGA (XC7A100T-1CSG324C). The results were derived following functional simulation and synthesis of the 128-bit AES encryption core. A. Functional Simulation The simulation was conducted using Vivado's integrated simulator. The design was evaluated with predetermined plaintext and key values to ensure the accuracy of the encryption process.

Test Vector:

Plaintext: 00112233445566778899AABBCCDDEEFF

Key: 000102030405060708090A0B0C0D0E0F

Expected Ciphertext:

69C4E0D86A7B0430D8CDB78070B4C55A

The simulation outcomes corresponded with the expected ciphertext, thereby confirming the functional accuracy. B. Synthesis Report The post-synthesis resource utilization for the AES encryption core is as follows:

Resource	Utilization
Look-Up Tables (LUTs)	3,216
Flip-Flops (FFs)	2,048
Block RAMs (BRAMs)	0
DSP Slices	0
Maximum Frequency	147 MHz
Latency	11 clock cycles

The design was optimized for both area and throughput without employing dedicated DSP slices or BRAMs. All logic was implemented using LUTs and FFs. C. Power Estimation Utilizing the Xilinx Power Estimator (XPE), the dynamic power consumption was approximated to be 110 mW, rendering it suitable for low-power embedded applications. D. Comparative Analysis In comparison to traditional software implementations, the hardware design achieves: ~15× faster throughput Constant-time execution (resistant to timing attacks) Enhanced energy efficiency in constrained environments.

Conclusion

This study presents the implementation of documents of advanced encryption algorithms (AES) using Verilog HDL on the Xilinx Vivado platform. Effective layout illustrations primary encryption processes, along with subbytes, moving, mixcolumns and addroundKey, are optimized to install FPGA. Simulation function verified the accuracy of encryption good judgment, while the synthesis effects indicate that the layout is powerful inside the vicinity and is able to operating at high frequency, which makes it ideal for included safety packages in actual time.

Way to the use of parallel and calendar can be anticipated by way of the device; this approach shows huge overall performance improvements in comparison to conventional software program password structures. The consequences of affirmation that AE can be efficaciously applied on FPGA

systems with confined assets whilst preserving protection and speed. In addition, the low power consumption of the design and minimum use of substances makes it very suitable for environmental restrained environments along with hand held gadget, iodine on the buttons on the board and protection sensor community. Successful synthesis without DSP or blocking off slices additionally illustrates the layout capacity of the layout in distinctive FPGA families and cases of use.

Future studies can consciousness at the AES interpreting, optimizing energy consumption or combining countermeasures in opposition to secondary channel attacks to decorate coding consider. The growth of this job to guide some AES modes (for instance, CBC, GCM, CTR) will even enhance its utility potential thru a bigger spectrum of secure protocols. In addition, the integration of dynamic control structures or trans -code -code (e.G. AES with RSA / ECC to trade security locks) can contribute to growing extra complete and resilient encryption frames for brand new technology protection communication systems.

References:

Research Papers:

1. S. Morioka and A. Satoh, "A 10-Gbps Full-AES Crypto Design with a Twisted-BDD S-Box Architecture," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E86-A, no. 1, pp. 54–63, Jan. 2003.
2. D. Ramakrishna and M. A. Shaik, "A Comprehensive Analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges," IEEE Access, vol. 13, pp. 11576–11594, Jan. 2025, doi: 10.1109/ACCESS.2024.3518533.
3. L. Ning, Y. Ali, H. Ke, S. Nazir, and Z. Huanli, "A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography Security Requirements for Internet of Health Things," IEEE Access, vol. 8, pp. 220165–220181, Dec. 2020, doi: 10.1109/ACCESS.2020.3041327.
4. A. H. Ali, E. K. Gbashi, H. Alaskar, and A. J. Hussain, "A Lightweight Image Encryption Algorithm Based on Secure Key Generation," IEEE Access, vol. 12, pp. 95871–95886, Jul. 2024, doi: 10.1109/ACCESS.2024.3414334.
5. A. Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig, and H. T. Elshoush, "A Polymorphic Advanced Encryption Standard – A Novel Approach," IEEE Access, vol. 9, pp. 20191–20202, Jan. 2021, doi: 10.1109/ACCESS.2021.3051556.
6. R. Kumar et al., "A Time-/Frequency-Domain Side-Channel Attack Resistant AES-128 and RSA-4K Crypto-Processor in 14-nm CMOS," IEEE Journal of Solid-State Circuits, vol. 56, no. 4, pp. 1141–1152, Apr. 2021, doi: 10.1109/JSSC.2021.3052146.
7. A. Cohen, R. G. L. D'Oliveira, K. R. Duffy, J. Woo, and M. Médard, "AES as Error Correction: Cryptosystems for Reliable Communication," IEEE Communications Letters, vol. 27, no. 8, pp. 1964–1967, Aug. 2023, doi: 10.1109/LCOMM.2023.3285404.
8. T. T. Luong, N. N. Cuong, and B. Vo, "AES Security Improvement by Utilizing New Key-Dependent XOR Tables," IEEE Access, vol. 12, pp. 53158–53170, Apr. 2024, doi:10.1109/ACCESS.2024.3387268.
9. C.-H. Wang, C.-L. Chuang, and C.-W. Wu, "An efficient multimode multiplier supporting AES and fundamental operations of public-key cryptosystems," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 18, no. 4, pp. 553–563, Apr. 2010, doi: 10.1109/TVLSI.2009.2013958.
10. P. Nannipieri, S. Di Matteo, L. Baldanzi, L. Crocetti, L. Zulberti, S. Saponara, and L. Fanucci, "VLSI design of advanced-features AES cryptoprocessor in the framework of the European Processor Initiative," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 2, pp. 177–186, Feb. 2022, doi: 10.1109/TVLSI.2021.3129107.
11. Y. Kim and S. C. Seo, "Efficient implementation of AES and CTR_DRBG on 8-bit AVR-based sensor nodes," IEEE Access, vol. 9, pp. 30496–30510, Feb. 2021, doi:10.1109/ACCESS.2021.3059623.
12. S. Abboud and N. Abdoun, "Enhancing LoRaWAN security: An advanced AES-based cryptographic approach," IEEE Access, vol. 12, pp. 2589–2604, Jan. 2024, doi:10.1109/ACCESS.2023.3348416.
13. M. Y. Shakor, M. I. Khaleel, M. Safran, S. Alfarhood, and M. Zhu, "Dynamic AES encryption and blockchain key management: A novel solution for cloud data security," IEEE Access, vol. 12, pp. 26334–26343, Jan. 2024, doi: 10.1109/ACCESS.2024.3351119.
14. S. Ahmed, N. Ahmad, N. A. Shah, G. E. M. Abro, A. Wijayanto, A. Hirsi, and A. R. Altaf, "Lightweight AES design for IoT applications: Optimizations in FPGA and ASIC with DFA countermeasure strategies," IEEE Access, vol. 13, pp. 22489–22506, Feb. 2025, doi:10.1109/ACCESS.2025.3533611.
15. K.-S. Chong, J.-S. Ng, J. Chen, N. K. Z. Lwin, N. A. Kyaw, W.-G. Ho, J. Chang, and B.-H. Gwee, "Dual-hiding side-channel-attack resistant FPGA-based asynchronous-logic AES: Design, countermeasures and evaluation," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 11, no. 2, pp. 343–355, June 2021, doi:10.1109/JETCAS.2021.3077887. J. Wu, "Prediction of hourly solar radiation with multi-model framework," 2013.