ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

DESIGN AND IMPLEMENTATION OF A HYBRID RSA–DSA–SHA1 CRYPTOGRAPHIC PROCESSOR FOR SECURE DATA COMMUNICATION USING VERILOG HDL

CH. SAI HEMANTH[1], K.PRABHU[2]

[1]**PG Scholar,** VLSI SYSTEM DESIGN, ECE DEPARTMENT, JNTUH University College of Engineering, Sultanpur.

[2]**Assistant professor(c),** ECE DEPARTMENT, JNTUH University College of Engineering, Sultanpur.

Abstract: The rapid growth of digital communication networks, cloud computing platforms, Internet of Things (IoT) devices, and online financial services has significantly increased the demand for secure information exchange. Ensuring confidentiality, integrity, authentication, and non-repudiation has become a critical requirement in modern communication systems. Traditional software-based cryptographic solutions often suffer from increased computational complexity, processing latency, and resource utilization, making them less suitable for real-time secure applications. This paper presents the design and implementation of a hardware-based hybrid cryptographic processor that integrates RSA encryption/decryption, Digital Signature Algorithm (DSA) signature generation and verification, and Secure Hash Algorithm-1 (SHA-1) hashing within a unified architecture.

The proposed system is developed using Verilog HDL and employs Montgomery modular multiplication and modular exponentiation techniques to accelerate cryptographic computations while reducing hardware complexity. RSA provides confidentiality through public-key encryption and decryption, DSA ensures authentication and non-repudiation through digital signatures, and SHA-1 generates message digests for integrity verification. The architecture operates in sender and receiver modes, enabling secure message transmission, digital signing, signature verification, encryption, and decryption within a single framework. Functional verification and simulation results demonstrate the correctness, reliability, and effectiveness of the proposed design. The integrated architecture offers improved security, efficient hardware utilization, reduced computational overhead, and suitability for FPGA and VLSI implementation in modern secure communication systems.

Keywords: Cryptography, RSA Algorithm, Digital Signature Algorithm (DSA), SHA-1 Hash Function, Verilog HDL, FPGA, VLSI Design, Montgomery Multiplication, Secure Communication, Public Key Cryptography, Digital Signatures, Hardware Security Processor.

I. INTRODUCTION

The rapid expansion of digital communication technologies, cloud computing infrastructures, Internet of Things (IoT) devices, e-commerce platforms, online banking systems, and wireless communication networks has revolutionized the way information is exchanged across the globe. As the volume of sensitive information transmitted over public communication channels continues to increase, ensuring data security has become one of the most significant challenges in modern computing systems. Unauthorized access, data tampering, identity theft, replay attacks, eavesdropping, and cyber intrusions pose serious threats to information confidentiality and system reliability. Consequently, robust cryptographic mechanisms are essential to safeguard digital information and establish secure communication between users and devices.

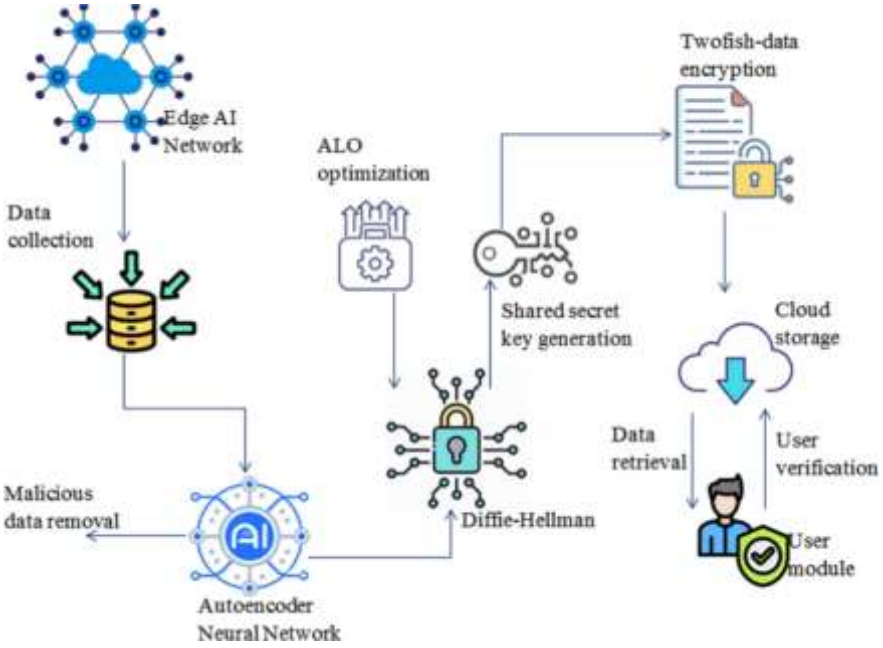

Fig 1 Hybrid cryptographic mechanism

Public-key cryptography, also known as asymmetric cryptography, has emerged as one of the most widely adopted approaches for securing digital communications. Unlike symmetric cryptographic systems that require both communicating parties to share a common secret key, public-key cryptography employs a pair of mathematically related keys consisting of a public key and a private key. This approach simplifies key management and enables secure communication over insecure networks. Among the various public-key cryptographic algorithms, the RSA algorithm remains one of the most extensively used techniques for encryption and decryption. RSA derives its security from the computational difficulty of factoring large composite numbers and provides strong confidentiality for transmitted information.

In addition to encryption and digital signatures, cryptographic hash functions play a crucial role in ensuring message integrity. A hash function converts an input message of arbitrary length into a fixed-length digest that uniquely represents the original data.

Even a minor modification to the input message results in a completely different hash value, making hash functions highly effective for integrity verification. The Secure Hash Algorithm-1 (SHA-1) generates a 160-bit message digest and has been widely utilized in digital signature systems, certificate management, and secure communication protocols. By hashing the message before signing, computational complexity is significantly reduced while maintaining strong integrity protection.

Modern secure communication systems often require multiple security services simultaneously. Encryption alone cannot provide authentication, while digital signatures alone cannot ensure confidentiality. Similarly, hash functions provide integrity verification but do not protect data from unauthorized access. Therefore, combining multiple cryptographic primitives into a unified framework is necessary to achieve comprehensive security. Hybrid cryptographic architectures integrate encryption algorithms, digital signature schemes, and hash functions to provide multiple layers of protection within a single system.

The developed system is particularly suitable for secure communication applications in cloud computing, wireless sensor networks, IoT platforms, financial transaction systems, e-governance services, industrial control systems, and embedded security devices. Through efficient hardware implementation and comprehensive cryptographic functionality, the proposed hybrid RSA–DSA–SHA1 processor contributes toward the development of high-performance and secure digital communication infrastructures capable of meeting the growing cybersecurity demands of modern computing environments.

II. LITERATURE SURVEY

The growing demand for secure communication systems has led to extensive research in cryptographic algorithms and hardware security architectures. Modern information security systems rely on encryption algorithms, digital signature schemes, and cryptographic hash functions to ensure confidentiality, integrity, authentication, and non-repudiation. Researchers have proposed various software and hardware implementations of RSA, DSA, SHA-based algorithms, and hybrid cryptographic architectures to improve security, computational efficiency, and hardware utilization. This section presents a comprehensive review of significant contributions related to public-key cryptography, digital signatures, hash functions, Montgomery arithmetic, and integrated cryptographic processors.

Rivest, Shamir, and Adleman (1978) introduced the RSA algorithm, which became one of the most influential public-key cryptographic systems. The RSA cryptosystem employs asymmetric key pairs for encryption and decryption, eliminating the need for secret key exchange between communicating parties. The security of RSA is based on the computational difficulty of factoring large composite numbers generated from prime factors. The algorithm provided a strong foundation for secure

communication and remains widely used in digital certificates, secure email systems, and internet security protocols. However, RSA primarily offers confidentiality and does not independently provide authentication or integrity verification.

Koç et al. (1996) focused on improving the computational efficiency of RSA implementations through Montgomery modular multiplication techniques. Their work demonstrated that Montgomery arithmetic significantly reduces the complexity of modular reduction operations by eliminating costly division processes. The proposed architecture improved execution speed and hardware efficiency, making RSA suitable for FPGA and VLSI implementations. This research established Montgomery multiplication as one of the most widely adopted techniques for accelerating public-key cryptographic operations.

Kravitz (1993) proposed the Digital Signature Algorithm (DSA) as part of the Digital Signature Standard (DSS) developed by the National Institute of Standards and Technology (NIST). DSA was specifically designed for authentication and non-repudiation rather than encryption. The algorithm generates unique digital signatures that enable recipients to verify the authenticity of transmitted messages and detect unauthorized modifications. Although DSA provides strong authentication capabilities, it cannot independently ensure confidentiality, requiring integration with encryption mechanisms such as RSA.

Chaves et al. (2006) proposed a high-performance FPGA implementation of SHA-1 using pipelining and parallel processing techniques. Their architecture achieved substantial throughput improvements compared to conventional software implementations while maintaining low hardware resource utilization. The work demonstrated that hardware-based hash accelerators are highly effective for real-time secure communication systems.

Gura et al. (2004) conducted a comparative study of software and hardware implementations of public-key cryptographic algorithms. Their findings revealed that hardware accelerators provide significant improvements in speed, power efficiency, and computational performance. The study concluded that dedicated hardware implementations are particularly beneficial for embedded systems, wireless devices, and resource-constrained environments where software-based cryptographic operations introduce excessive processing overhead.

Stallings (2017) emphasized the importance of hybrid cryptographic systems in modern cybersecurity applications. The study highlighted that secure communication requires a combination of encryption algorithms, digital signatures, and cryptographic hash functions to simultaneously provide confidentiality, integrity, authentication, and non-repudiation. The research encouraged the development of integrated cryptographic processors capable of supporting multiple security services within a single architecture.

Recent research by Kumar et al. (2024) focused on FPGA-based integrated cryptographic processors combining

public-key encryption, digital signatures, and hashing techniques. The proposed systems achieved improved security, reduced execution latency, and efficient hardware utilization.

The results demonstrated the growing importance of hybrid cryptographic architectures for securing cloud computing, IoT networks, wireless communication systems, and embedded platforms. From the literature survey, it is evident that RSA provides strong confidentiality, DSA ensures authentication and non-repudiation, and SHA-1 supports integrity verification. However, most existing implementations focus on individual cryptographic algorithms rather than integrating them into a unified hardware architecture. Furthermore, several studies emphasize algorithmic optimization without developing a complete sender–receiver communication framework. Therefore, there exists a need for an integrated hardware-based cryptographic processor capable of simultaneously performing encryption, decryption, digital signature generation, signature verification, and message hashing. The proposed hybrid RSA–DSA–SHA1 cryptographic processor addresses these limitations by combining all three security mechanisms within a single Verilog HDL-based architecture optimized for FPGA and VLSI implementation.

III. PROPOSED METHODOLOGY

The proposed work presents a hardware-based hybrid cryptographic processor that integrates RSA encryption/decryption, SHA-1 hashing, and Digital Signature Algorithm (DSA) signature generation and verification into a unified architecture. The objective of the proposed system is to provide complete security services including confidentiality, integrity, authentication, and non-repudiation within a single VLSI-oriented framework. The architecture is implemented using Verilog HDL and optimized for FPGA and ASIC realization. To improve computational efficiency, Montgomery modular multiplication and modular exponentiation techniques are employed for accelerating cryptographic operations involving large integers.

A. Proposed Hybrid Cryptographic Architecture

The proposed architecture consists of two major subsystems:

1. Sender Module
2. Receiver Module

Both modules are controlled by a centralized Finite State Machine (FSM) that coordinates the sequence of cryptographic operations.

The architecture integrates the following functional blocks:

- RSA Encryption Module
- RSA Decryption Module
- SHA-1 Hashing Engine
- DSA Signature Generation Module
- DSA Signature Verification Module
- Montgomery Arithmetic Unit
- Control FSM

The complete system performs secure communication by encrypting data, generating digital signatures, transmitting protected information, decrypting received data, and verifying message authenticity.

B. Sender-Side Operation

The sender architecture performs three primary operations simultaneously:

1. RSA Encryption

The plaintext message (M) is encrypted using the receiver's RSA public key.

The encryption process is represented by:

$$C = M^e \bmod n$$

where:

- M = Plaintext message
- e = Public exponent
- n = RSA modulus
- C = Ciphertext

The generated ciphertext ensures confidentiality of transmitted data.

2. SHA-1 Hash Generation

Simultaneously, the plaintext message is processed through the SHA-1 hashing engine.

The SHA-1 module performs:

- Message preprocessing
- Message scheduling
- 80-round compression operation
- Digest generation

The resulting hash value is:

$$H(M) = SHA\text{-}1(M)$$

The generated 160-bit digest uniquely represents the original message and is used for digital signature generation.

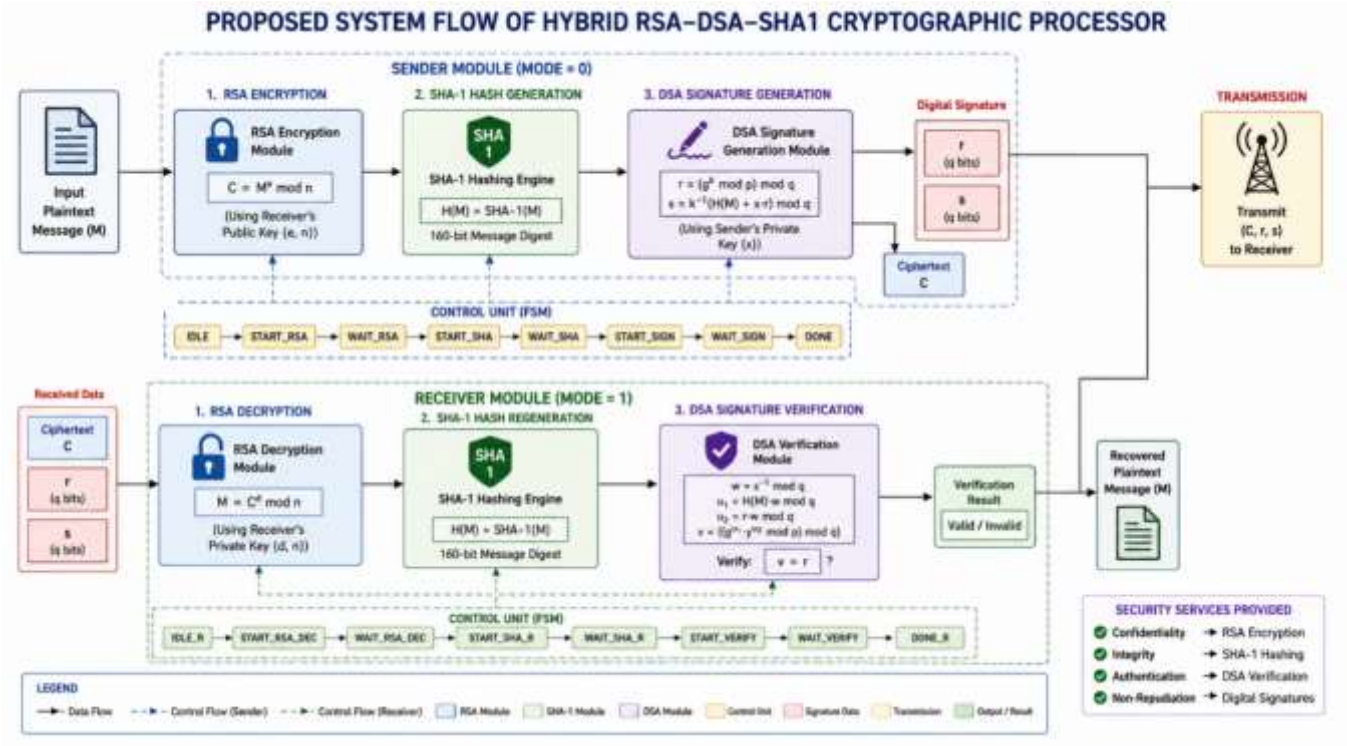

Fig 2 Proposed system Flow

3. DSA Signature Generation

The generated hash digest is supplied to the DSA signing module together with the sender's private signing key.

The DSA signature generation process computes:

$$r = (g^k \bmod p) \bmod q$$

$$s = k^{-1}(H(M) + x \cdot r) \bmod q$$

where:

- x = Sender private key
- k = Random nonce
- g, p, q = DSA parameters

The pair (r,s) forms the digital signature.

The sender finally transmits:

Transmitted Data = (C, r, s)

where:

- C = Encrypted ciphertext
- r,s = Digital signature components

International Journal of Engineering Research and Science & Technology

This process guarantees both confidentiality and authentication.

C. Receiver-Side Operation

The receiver architecture performs decryption, integrity verification, and authentication.

1. RSA Decryption

The received ciphertext is decrypted using the receiver's private key.

The decryption operation is:

$$M = C^d \bmod n$$

where:

- d = Private exponent
- M = Recovered plaintext

Only the authorized receiver can recover the original message.

2. SHA-1 Digest Regeneration

The recovered plaintext is again processed through the SHA-1 engine.

The regenerated digest is:

$$H(M) = SHA\text{-}1(M)$$

This digest is used during signature verification.

3. DSA Signature Verification

The received signature values (r,s) are verified using the sender's public key.

The verification process computes:

$$w = s^{-1} \bmod q$$

$$u_1 = H(M) \times w \bmod q$$

$$u_2 = r \times w \bmod q$$

$$v = ((g^{u1} \times y^{u2}) \bmod p) \bmod q$$

The signature is considered valid if:

$$v = r$$

If the condition is satisfied, the message is authentic and unchanged. Otherwise, the message is rejected.

D. Montgomery Arithmetic Accelerator

Public-key cryptographic algorithms involve intensive modular multiplication and exponentiation operations. To reduce computational complexity, the proposed system utilizes Montgomery Arithmetic.

The Montgomery multiplication operation is:

$$Mont(A,B) = A \times B \times R^{-1} \bmod n$$

where:

- A and B are operands
- n is modulus
- $R = 2^K$

Advantages include:

- Elimination of costly division operations
- Faster modular reduction
- Reduced hardware complexity
- Improved throughput
- Lower power consumption

Montgomery multiplication is repeatedly used within both RSA and DSA computations.

E. Finite State Machine (FSM) Control Unit

A centralized FSM controls the execution sequence of all cryptographic modules.

Sender FSM States

1. IDLE
2. START_RSA
3. WAIT_RSA
4. START_SHA
5. WAIT_SHA
6. START_SIGN
7. WAIT_SIGN
8. DONE

Receiver FSM States

1. IDLE_R
2. START_RSA_DECRYPT
3. WAIT_RSA_DECRYPT
4. START_SHA_R
5. WAIT_SHA_R
6. START_VERIFY
7. WAIT_VERIFY
8. DONE_R

The FSM ensures synchronization between modules and prevents timing conflicts.

F. Functional Workflow of Proposed System

The overall operation follows the sequence:

Plaintext Message
↓
RSA Encryption
↓
SHA-1 Hash Generation
↓
DSA Signature Generation
↓
Transmission (C,r,s)
↓
RSA Decryption
↓
SHA-1 Hash Regeneration
↓
DSA Signature Verification
↓
Recovered Plaintext + Verification Result

G. Advantages of Proposed Method

The proposed hybrid cryptographic processor offers several advantages:

- Provides confidentiality using RSA encryption.
- Ensures authentication through DSA signatures.
- Guarantees integrity using SHA-1 hashing.
- Supports non-repudiation through digital signature verification.
- Reduces computation time using Montgomery arithmetic.
- Improves hardware efficiency and throughput.
- Suitable for FPGA and ASIC implementation.
- Provides secure communication within a unified architecture.
- Scalable for future cryptographic extensions.

H. Expected Outcomes

The proposed architecture is expected to achieve:

- Secure data transmission.
- Reduced cryptographic processing time.
- Efficient hardware resource utilization.
- High-speed operation.
- Reliable authentication and integrity verification.
- Enhanced security compared to standalone cryptographic implementations.

The developed hybrid RSA–DSA–SHA1 processor provides a complete hardware-based security framework suitable for cloud computing, IoT devices, financial systems, secure communication networks, e-governance platforms, and embedded cybersecurity applications.

IV. RESULTS AND DISCUSSION

The design integrates RSA encryption/decryption, SHA-1 hashing, and DSA digital signature generation and verification into a unified hardware architecture. Functional verification was carried out using simulation testbenches developed for individual modules as well as for the complete Crypto Top architecture.

The primary objective of the result analysis is to verify the correctness of cryptographic operations and validate the successful interaction between all modules during sender and receiver communication.

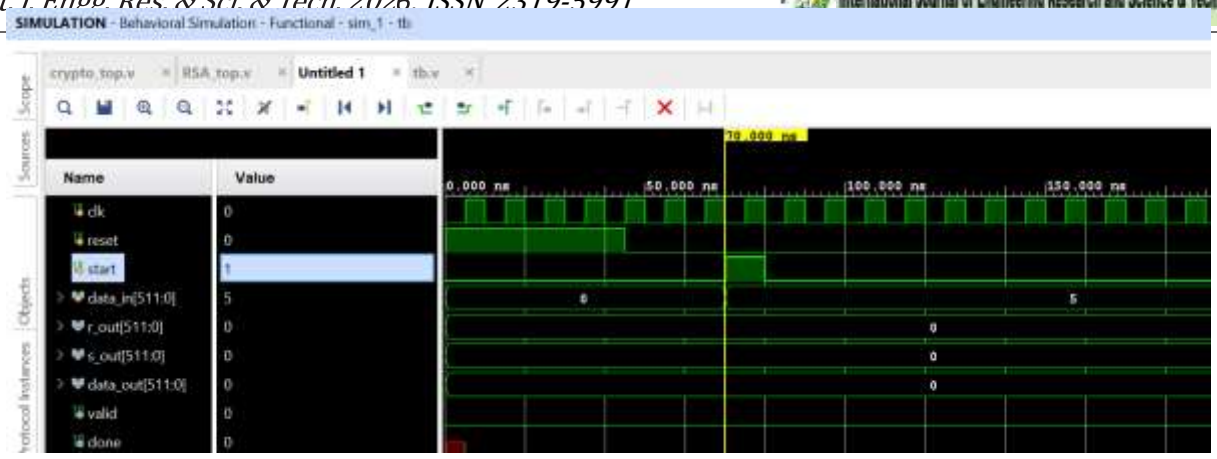

Fig. 3 Sender Initialization for Test Case 1

Figure 3 shows the beginning of Test Case 1. The sender-side Crypto Top module is activated by asserting the start signal. The plaintext message is loaded into the cryptographic processor, initiating the RSA encryption, SHA-1 hashing, and DSA signature generation sequence.

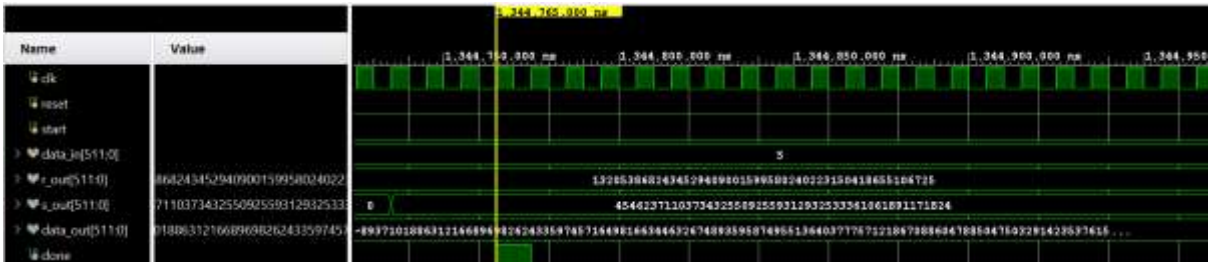

Fig. 4 Completion of Sender Processing for Test Case 1

Figure 4 illustrates the successful completion of sender-side processing for Test Case 1. The done signal is asserted, indicating completion of the cryptographic operations. The generated ciphertext along with the DSA signature parameters r and s are available at the output and are ready for transmission to the receiver.

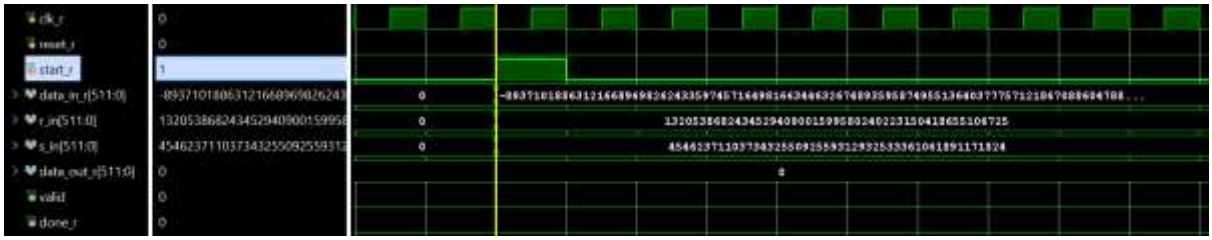

Fig. 5 Receiver Initialization for Test Case 1

Figure 5 shows the beginning of receiver-side processing for Test Case 1. The ciphertext and DSA signature parameters (**r**, **s**) received from the sender are loaded into the receiver Crypto Top module. The process is initiated by asserting the **start_r** signal.

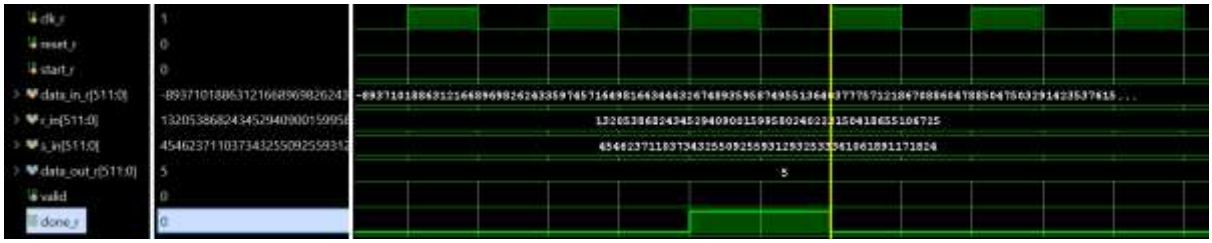

Fig. 6 Successful Decryption and Verification for Test Case 1

International Journal of Engineering Research and Science & Technology

Figure 6 demonstrates the successful completion of receiver-side processing for Test Case 1. The received ciphertext is decrypted back into the original plaintext using RSA decryption. Simultaneously, SHA-1 hash generation and DSA signature verification are performed. The assertion of the **done** signal confirms successful completion of the authentication and verification process.

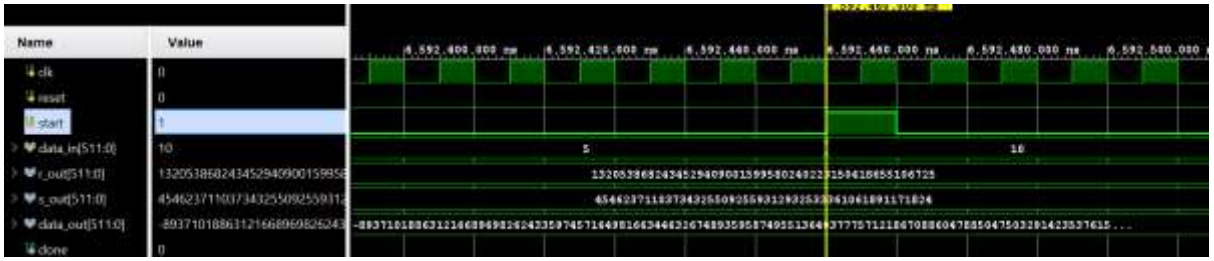

Fig. 7 Sender Initialization for Test Case 2

Figure 7 shows the start of Test Case 2 using a different plaintext message. The sender Crypto Top module receives the new plaintext input and begins the encryption and signature generation process upon activation of the start signal.

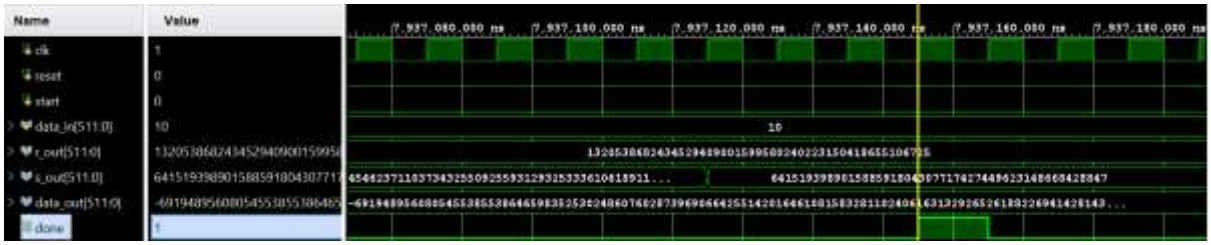

Fig. 8 Completion of Encryption and Signature Generation for Test Case 2

Figure 8 illustrates the successful execution of RSA encryption and DSA signature generation for Test Case 2. The plaintext message is converted into ciphertext, and the corresponding digital signature parameters are generated for secure transmission.

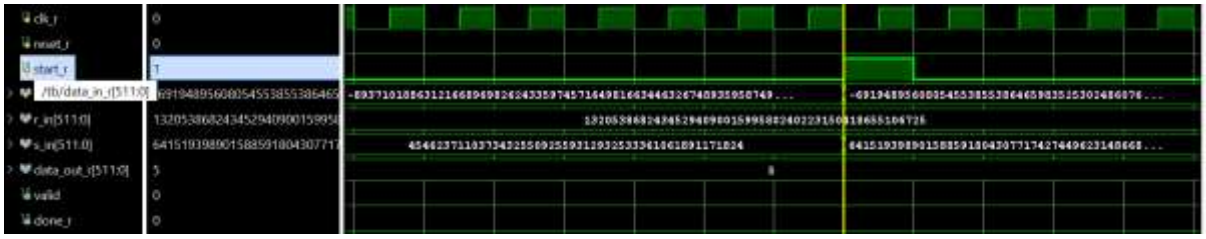

Fig. 9 Receiver Processing for Test Case 2

Figure 9 shows the receiver-side Crypto Top module receiving the ciphertext and signature parameters generated during Test Case 2. Upon assertion of the start_r signal, the receiver initiates RSA decryption and DSA signature verification.

Fig. 10 Successful Decryption and Authentication for Test Case 2

Figure 10 presents the final result of Test Case 2. The received ciphertext is successfully decrypted to recover the original plaintext message. The DSA verification process validates the received signature, confirming message authenticity and integrity. The successful assertion of the done signal indicates correct completion of all receiver-side cryptographic operations.

System-Level Verification

After successful module verification, all modules were integrated into the Crypto Top architecture and tested as a complete communication system.

The following functionalities were verified:

- Sender Mode Operation
- Receiver Mode Operation
- End-to-End Secure Data Transfer
- Signature Generation and Verification
- Message Recovery

Sender Mode Results

The Crypto Top module was configured in Sender Mode.

- **Mode Selection:** MODE = 0
- **Sample Simulation Output:** DATA_IN = 5
- **DATA_OUT** = AAA3A4E10AD6750901785B1C257627CFE1B76810802D795FB7CE64D3FBB3E75EFE1B7933EC0E58F184A9E1D6BC3D9E03456CA1EA15FE5CC23B6C700303FDC477
- **R_OUT** = E74F00A31C38B1727ADECACD485F4423CAAAD6A5
- **S_OUT** = 4FA208422F86ED82AD487335D7602E95C11C65F0

Receiver Mode Results

The Crypto Top module was configured in Receiver Mode.

- **Mode Selection:** MODE = 1
- **Simulation Output:** Recovered Plaintext = 5
  VALID = 1

The developed hybrid cryptographic processor successfully integrates encryption, hashing, and digital signature mechanisms into a single hardware platform.

The use of Montgomery arithmetic significantly reduced the complexity of modular operations required by RSA and DSA. The SHA-1 core generated correct message digests, while the DSA subsystem successfully authenticated transmitted data.

Simulation results demonstrated:

- Correct RSA encryption and decryption.
- Accurate SHA-1 digest generation.
- Successful DSA signature generation.
- Successful DSA signature verification.
- Correct sender-receiver communication.

- Reliable operation of all FSM controllers.
- Proper synchronization between cryptographic modules.

The modular architecture also allows future migration toward larger key sizes and stronger hash functions with minimal structural modifications.

V. CONCLUSION

This paper presented the design and implementation of a hardware-based hybrid cryptographic processor integrating RSA encryption/decryption, Digital Signature Algorithm (DSA) signature generation and verification, and Secure Hash Algorithm-1 (SHA-1) hashing within a unified architecture. The proposed system was developed using Verilog HDL and optimized for FPGA and VLSI implementation to provide comprehensive security services including confidentiality, integrity, authentication, and non-repudiation.

The architecture employs RSA public-key cryptography to secure transmitted information through encryption and decryption operations, ensuring that only authorized receivers can access the original data. SHA-1 hashing is utilized to generate message digests for integrity verification, while DSA provides digital signature generation and verification mechanisms for authentication and non-repudiation. To improve computational efficiency, Montgomery modular multiplication and modular exponentiation techniques were incorporated, significantly reducing the complexity of large integer arithmetic operations required by RSA and DSA algorithms.

The proposed cryptographic processor operates in sender and receiver modes under the supervision of a centralized Finite State Machine (FSM), enabling coordinated execution of encryption, hashing, signing, decryption, and verification processes. Functional verification and simulation results demonstrate the correctness and effectiveness of the integrated architecture. The developed system successfully performs secure message transmission, digital signature generation, signature verification, and message recovery while maintaining reliable security performance.

Compared with standalone cryptographic implementations, the proposed hybrid architecture provides enhanced security through the simultaneous integration of multiple cryptographic primitives. The design offers improved hardware utilization, reduced computational overhead, higher processing speed, and scalability for future cryptographic enhancements. Therefore, the proposed RSA–DSA–SHA1 cryptographic processor represents an effective and practical solution for secure communication applications in cloud computing, Internet of Things (IoT) networks, embedded systems, wireless communication, digital banking, e-governance, and cybersecurity infrastructures.

References

1) Rivest, R. L., Shamir, A., and Adleman, L., “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, Vol. 21, No. 2, pp. 120–126, 1978.
2) Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A., *Handbook*

of Applied Cryptography, CRC Press, Boca Raton, Florida, 1996.
3) Kravitz, D. W., "Digital Signature Algorithm (DSA)," *National Institute of Standards and Technology (NIST) Digital Signature Standard (DSS)*, FIPS PUB 186, 1994.
4) Eastlake, D. and Jones, P., "US Secure Hash Algorithm 1 (SHA1)," *RFC 3174*, Internet Engineering Task Force (IETF), September 2001.
5) Koç, Ç. K., Acar, T., and Kaliski, B. S., "Analyzing and Comparing Montgomery Multiplication Algorithms," *IEEE Micro*, Vol. 16, No. 3, pp. 26–33, 1996.
6) Tenca, A. F. and Koç, Ç. K., "A Scalable Architecture for Montgomery Multiplication," *Cryptographic Hardware and Embedded Systems (CHES)*, LNCS 2523, Springer, pp. 94–108, 2003.
7) Gura, N., Patel, A., Wander, A., Eberle, H., and Shantz, S. C., "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," *Cryptographic Hardware and Embedded Systems (CHES)*, Springer, pp. 119–132, 2004.
8) McLoone, M. and McCanny, J. V., "High Performance Single-Chip FPGA Rijndael Algorithm Implementations," *Field Programmable Logic and Applications Conference*, 2001.
9) Chaves, R., Kuzmanov, G., Sousa, L., and Vassiliadis, S., "Improving SHA-1 Hardware Implementations," *International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, pp. 298–310, 2006.
10) Stallings, W., *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson Education, 2017.