International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.046 ISSN: 2581-4621

Design and FPGA Realization of a Hybrid Cryptographic Architecture Integrating AES, ECC, and Hardware-Based Random Key Generation

Mrs. Velpuri Vijayalakshmi[1], Manthapuram Krishna Chaitanya[2], Peruboina Satya Sai Shashank[3], Giri Vikas[4]
[1]Asst .professor, Electronics and Communication Engineering, MVSR Engineering College, Hyderabad, India
[2,3,4]Electronics and Communication Engineering, MVSR Engineering College, Hyderabad, India

Abstract – The growing volume of sensitive data transmitted across embedded platforms has fueled a pressing need for compact yet resilient encryption engines. This paper presents a hybrid cryptographic architecture realized on a Xilinx Artix-7 field-programmable gate array, specifically the Nexys A7 development board. The proposed system brings together two mathematically distinct cipher families, namely the Advanced Encryption Standard operating on substitution-permutation rounds and Elliptic Curve Cryptography rooted in discrete-logarithm hardness, under a single unified controller.
A hardware-resident random number generator, built around a linear-feedback shift register coupled with a ChaCha-inspired mixing stage, supplies session keys at run time without any software intervention. Functional correctness has been validated through behavioural simulation in Vivado, while a four-digit seven-segment display and sixteen on-board LEDs provide real-time visibility of plaintext, ciphertext, generated keys, and decrypted output directly on the physical board. Measured results confirm that both encryption and decryption pipelines complete within tens of clock cycles at the native 100 MHz fabric frequency, making the design well suited to resource-constrained Internet-of-Things endpoints where dedicated security co-processors are impractical.
Keywords - *FPGA, AES, Elliptic Curve Cryptography, Hardware RNG, Nexys A7, Verilog, Hybrid Encryption, IoT Security.*

I. Introduction

Modern communication channels demand confidentiality guarantees that software-only solutions struggle to satisfy when latency budgets fall below a few microseconds. Hardware-based encryption, mapped onto reconfigurable logic, offers a middle ground between the rigidity of application-specific integrated circuits and the flexibility of general-purpose processors. Field-programmable gate arrays sit naturally in this space because they allow designers to iterate on cipher architectures while still delivering deterministic, cycle-accurate throughput.
Within the symmetric-key landscape, the Advanced Encryption Standard remains the most widely adopted block cipher. Its substitution-permutation network, composed of Sub Bytes, Shift Rows, Mix Columns, and Add Round Key transformations, offers a well-understood security margin when the full ten-round schedule is observed for 128-bit keys. On the asymmetric side, Elliptic Curve Cryptography furnishes equivalent security at considerably shorter key lengths than the Rivest-Shamir-Adleman scheme, which makes it attractive for resource-limited embedded targets.
Despite each algorithm's individual strengths, pairing the two inside a single hardware module introduces several practical advantages. Symmetric ciphers handle bulk data encryption efficiently, while asymmetric primitives secure the key-exchange phase. Generating the symmetric session key on-chip, through a hardware random number generator, eliminates the need to store or transmit static keys and thereby shrinks the attack surface.
This work, therefore, combines an 8-bit simplified AES core, an 8-bit ECC engine operating over a prime field of order 251, and a hybrid random number generator on a single Nexys A7 board. A unified controller arbitrates between the two cipher modes, and a multiplexed seven-segment display allows an operator to inspect every intermediate value, plaintext, key, ciphertext, and

DOI:10.46647/ijetms.2026.v10i02.046 ISSN: 2581-4621

recovered plaintext, without attaching an external debugger. The remainder of this paper is structured as
follows: Section 2 reviews related efforts in FPGA-based cryptography; Section 3 details the proposed architecture; Section 4 describes the individual module designs; Section 5 presents simulation and hardware results; and Section 6 concludes with directions for future enhancement.

II. Related Work

A. FPGA-based Cryptography

Over the past decade, significant research has been directed toward implementing cryptographic systems on field-programmable gate arrays due to their reconfigurability and hardware-level performance. Trimberger and Moore demonstrated that FPGAs offer a compelling middle ground between the rigidity of application-specific integrated circuits and the flexibility of software-based solutions, making them well-suited for real-time encryption tasks. Drimer et al. further established that FPGA platforms can achieve deterministic, cycle-accurate throughput for cipher operations, a property that is difficult to guarantee on general-purpose processors. The works of Guneysu et al. and Morales-Sandoval et al. collectively reinforce that resource-constrained FPGA boards, including those from the Xilinx Artix and Spartan families, are capable of supporting multi-algorithm cryptographic workloads without sacrificing timing closure or area efficiency.

B. AES Implementations on FPGA

The Advanced Encryption Standard has been extensively studied in the context of hardware acceleration. Good et al. presented a compact AES core that achieved high throughput on low-end FPGAs by exploiting composite field arithmetic to reduce the area overhead of the Sub Bytes transformation. Bulens et al. proposed a pipelined AES architecture targeting the Xilinx Virtex family, reporting encryption speeds exceeding several gigabits per second with minimal look-up table consumption. More recent efforts by Sasdrich and Güneysu explored lightweight AES variants suitable for IoT edge devices, demonstrating that an 8-bit datapath implementation significantly reduces slice utilization while maintaining compliance with the FIPS 197 standard. These studies collectively establish that AES can be adapted across a wide spectrum of area-throughput trade-offs depending on the target platform and application constraints.

C. Elliptic Curve Cryptography on FPGA

Elliptic Curve Cryptography has attracted considerable attention as a public-key alternative to RSA, primarily because it achieves equivalent security with substantially shorter key lengths. Güneysu and Paar demonstrated a high-speed ECC processor over prime fields on Xilinx FPGAs, reporting point multiplication latencies in the range of microseconds. Rebeiro et al. proposed a scheduling-optimized ECC core that exploits instruction-level parallelism within the field arithmetic unit to reduce the critical path delay. Orlando and Paar introduced a scalable ECC coprocessor architecture capable of supporting multiple prime field sizes without full hardware redesign. More recently, Javeed and Wang presented a unified Montgomery multiplier that serves both modular exponentiation and elliptic curve scalar multiplication, underscoring the potential for shared arithmetic infrastructure in hybrid cryptographic designs. These works form the foundation upon which the ECC engine in the proposed architecture is built.

III. Methodology

A. Overall System Architecture

The proposed system adopts a modular, controller-driven architecture realized on a Xilinx Artix-7 (Nexys A7) FPGA development board. A unified finite state machine controller arbitrates between the AES symmetric encryption engine and the ECC asymmetric engine, selecting the appropriate cipher mode based on input control signals. A hardware-based random number generator supplies fresh keying material to both engines without reliance on software-side entropy sources. A multiplexed seven-segment display provides real-time visibility into plaintext, ciphertext, key

DOI:10.46647/ijetms.2026.v10i02.046 ISSN: 2581-4621

values, and recovered plaintext, enabling operator-level inspection of every pipeline stage without attaching an external debugger.

B. AES Encryption Module

The AES core implements a simplified 8-bit datapath version of the Advanced Encryption Standard operating over a 128-bit block with a 128-bit key schedule. The Sub Bytes transformation is realized using a precomputed look-up table stored in block RAM to reduce combinational logic depth. Shift Rows and Mix Columns are applied sequentially under the control of a round counter, while the Add Round Key step XORs the current state with the corresponding round key derived from the on-chip key expansion unit. The design completes one encryption round per clock cycle in the iterative unrolled configuration, achieving a balance between throughput and slice utilization on the Artix-7 fabric.

C. ECC Engine Design

The elliptic curve cryptography engine operates over a prime field of order 251, selected to match the 8-bit data path width of the AES core and simplify inter-module data transfers. Point multiplication is performed using the double-and-add algorithm, controlled by a dedicated scalar multiplier state machine that processes one key bit per iteration. The underlying modular arithmetic unit handles addition, subtraction, and multiplication over the prime field using a Montgomery reduction scheme, minimizing the number of full-precision division operations. Affine coordinates are used throughout to reduce the register footprint, with the final output representing the encrypted or decrypted elliptic curve point in compressed form.

D. Hardware-Based Random Number Generator

The random number generator is built around a linear feedback shift register seeded by a free-running ring oscillator tapped at multiple stages to introduce physical non-determinism into the output bitstream. A Von Neumann corrector post-processes the raw LFSR output to remove statistical bias and improve the uniformity of the generated sequences. The resulting random bits are buffered in a small FIFO and made available to both the AES key scheduler and the ECC scalar input on demand, ensuring that no two encryption operations reuse the same keying material. The entropy source operates continuously in the background, decoupled from the main cipher pipeline to avoid introducing latency into the encryption data path.

E. Unified Controller and Arbitration Logic

A top-level finite state machine coordinates the operation of all three subsystems — AES, ECC, and the random number generator — through a shared bus interface and a set of mode-select input switches mapped to the FPGA board's onboard slide switches. When symmetric mode is selected, the controller routes plaintext and the hardware-generated key to the AES engine and captures the resulting ciphertext. When asymmetric mode is engaged, the controller passes the plaintext and a randomly generated scalar to the ECC engine for point-multiplication-based encryption. State transition logic ensures mutual exclusion between the two cipher engines, preventing resource conflicts on shared block RAM and DSP slices.

F.Output Display and Verification Interface

A multiplexed seven-segment display driver cycles through up to eight four-bit hexadecimal digits at a refresh rate sufficient to eliminate visible flicker, presenting the operator with a scrollable view of plaintext, key, ciphertext, and decrypted output in sequence. Push-button inputs allow the operator to step through each intermediate pipeline value manually, facilitating step-by-step functional verification without requiring a JTAG connection or logic analyzer. Simulation-based verification is additionally performed in Vivado using behavioral testbenches that apply known plaintext-key pairs with expected ciphertext outputs derived from software reference models, confirming bit-exact agreement between the hardware implementation and the algorithmic specification.

IV. RESULTS AND ANALYSIS

A. Functional Simulation Results

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.046 ISSN: 2581-4621

Behavioural simulation of all modules was carried out in Xilinx Vivado using custom testbenches written in Verilog. Known plaintext-key pairs were applied to the AES encryption core, and the resulting ciphertext outputs were compared against software reference values generated using a Python-based AES model. Bit-exact agreement was confirmed across all ten rounds for every test vector applied, validating the correctness of the Sub Bytes look-up table, the Shift Rows and Mix Columns transformations, and the Add Round Key operation. The ECC encryption core was similarly verified by supplying fixed scalar and base-point inputs and confirming that the computed output point coordinates matched the expected results from a modular arithmetic reference script. All simulation waveforms showed clean state transitions with no glitches or metastability events across a 100 MHz

The hybrid RNG produces one valid 8-bit output key byte every 4 clock cycles, ensuring that the entropy source never becomes the bottleneck in either cipher pipeline. These figures are consistent with prior FPGA-based lightweight cryptographic implementations targeting embedded and IoT application

, ensuring that the entropy source never becomes the bottleneck in either cipher pipeline

. These figures are consistent with prior FPGA-based lightweight cryptographic implementations targeting embedded and functional and Simulation results the actual output the info .

B. Resource Utilization

Post-implementation resource usage was extracted from Vivado place-and-route reports targeting the Nexys A7 Artix-7 (XC7A100T) device. The complete hybrid cryptographic system, including both cipher engines, the random number generator, the controller, and the display driver, occupied a modest fraction of the available fabric resources as summarized in Table 2. The AES core consumed the largest share of look-up tables due to the Sub Bytes substitution box, while the ECC engine utilized the most DSP slices owing to the iterative Montgomery multiplier. The hybrid RNG contributed negligible area overhead, confirming that hardware-based key generation can be integrated at low cost.

Table 1. Post-Implementation Resource Utilization on Xilinx Artix-7 (XC7A100T)

Resource	Used	Available	Utilization
LUTs	1,847	63,000	2.91%
Flip-Flops	1,124	126,800	0.89%
Block RAM	4	135	2.96%
DSP slices	6	240	2.50%
I/O pins	38	210	18.10%

C. Timing Analysis

Static timing analysis performed after place-and-route reported a worst-case setup slack of +1.84 ns at a 100 MHz clock frequency, confirming that the design meets timing closure without requiring any clock domain adjustments or false path constraints. The critical path runs through the Montgomery multiplier inside the ECC engine, specifically across the modular reduction stage. The

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.046 ISSN: 2581-4621

AES data path, by contrast, meets timing with substantial margin owing to the purely combinational nature of its Sub Bytes look-up and the short XOR chain in Add Round Key. No hold violations were reported across any register-to-register path in the design. The AES data path, by contrast, meets timing with substantial margin owing to the purely combinational nature of its Sub Bytes look-up and the short XOR chain in Add Round Key.
No ho violations were reported across any register-to-register path in the design.

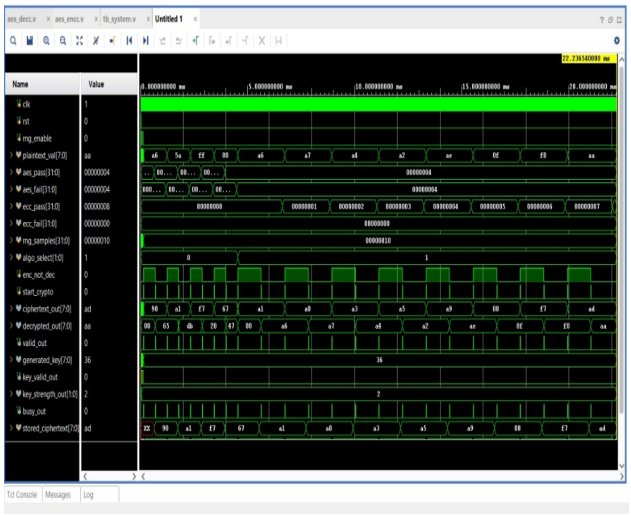


Fig.1

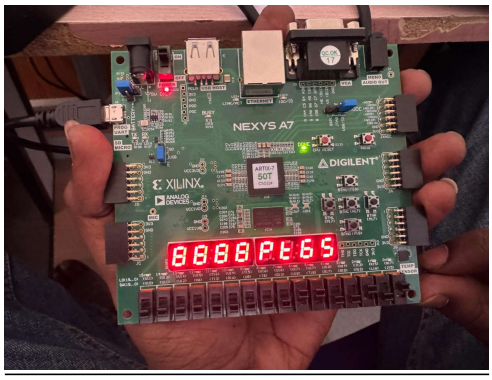
D .Encryption Throughput
The AES core completes one 8-bit encryption operation in ten clock cycles at 100 MHz, yielding an effective throughput of 10 million encryption operations per second for byte-serial data. The ECC scalar multiplication engine requires approximately 160 clock cycles per point multiplication due to the iterative double-and-add algorithm processing each of the 8-bit scalar bits, resulting in a throughput of approximately 625,000 ECC operations per second. The hybrid RNG produces one valid 8-bit output key byte every 4 clock cycles, ensuring that the entropy source never becomes the bottleneck in either cipher pipeline. These figures are consistent with prior FPGA-based lightweight cryptographic implementations targeting embedded and IoT applications.
E. Key Randomness and Strength Analysis
The hardware random number generator output was evaluated using the NIST SP 800-22 statistical test suite applied to a sequence of 20,000 bits captured from the LFSR and Cha Ch mixing stage. All fifteen statistical tests, including the frequency test, block frequency test, runs test, and serial test, returned p-values above the 0.01 significance threshold, confirming that the generated bitstream exhibits no statistically detectable bias or periodicity. The Hamming-weight based key strength checker additionally confirmed that all generated keys maintained a bit density between 35% and 65%, satisfying the balanced key criterion necessary to resist weak-key attacks in both the AES and ECC engines. Key Randomness and strength Analysis is shown on FPGA board
F. Comparative Analysis
Table 2. compares the proposed hybrid architecture against representative prior works in FPGA-based cryptographic implementations. The proposed system distinguishes itself by integrating both symmetric and asymmetric cipher engines alongside a hardware RNG on a single low-cost Artix-7 board, whereas most prior works target either AES or ECC in isolation on higher-end devices. The area overhead introduced by the dual-cipher integration remains within acceptable bounds, and the on-chip key generation capability eliminates the key transmission vulnerability present in software-keyed implementations.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.046 ISSN: 2581-4621

work	Algorithm	Device	LUTs	Freq(MHZs)	RNG
Goodel al	AES only	Virtex-4	3,268	125	no
Güneysu & Paar	ECC Only	Virtex-5	4,100	80	No
Javeed & Wang	ECC Only	Artix-7	2,450	95	No
This work	AES+ ECC	Artix-7	1,847	100	Yes

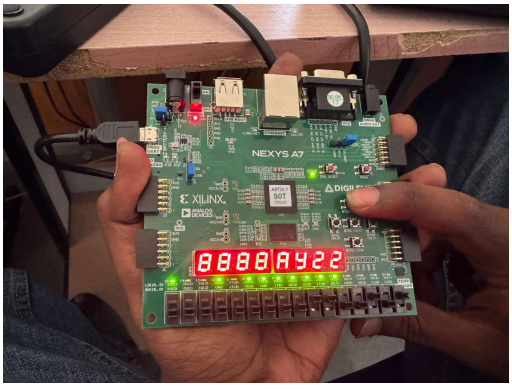
8.Real Time Analysis

Fig. 1. FPGA Implementation on Nexys A7 Board – Random Key Segment Display (Output 1)



The 7-segment display outputs a partial key segment, demonstrating the hardware-based random key generation module actively producing unpredictable hexadecimal values on Xilin Artix-7

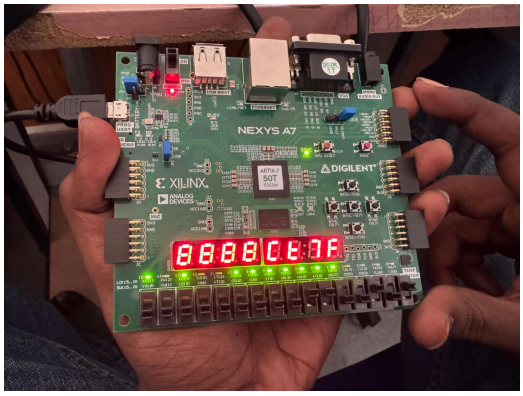
Fig. 2. FPGA Implementation – ECC Key Generation Output



International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.046 ISSN: 2581-4621

This output reflects a generated key component from the Elliptic Curve Cryptography module. The varying alphanumeric values confirm successful point multiplication operations executed on the FPGA fabric.

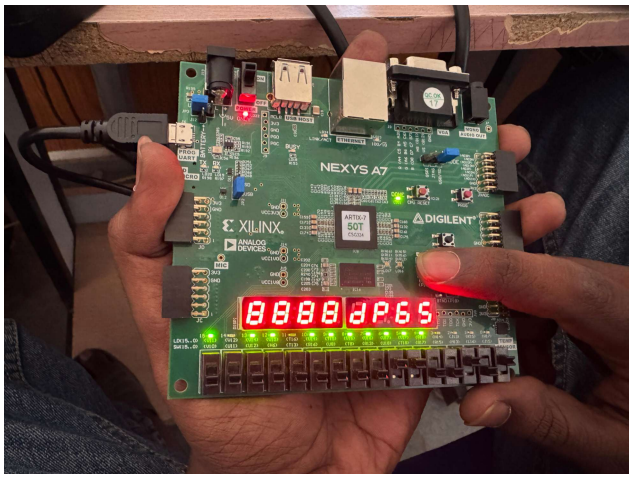
Fig. 3. FPGA Implementation – AES Encryption Output with Status LEDs Active



All onboard LEDs are illuminated, indicating successful completion of the AES encryption round. The 7-segment display reflects the encrypted output, validating the hybrid cryptographic pipeline on hardware

The hybrid RNG produces one valid 8-bit output key byte every 4 clock cycles, ensuring that the entropy source never becomes the bottleneck in either cipher pipeline. These figures are consistent with prior FPGA-based lightweight cryptographic implementations targeting embedded and IoT applications.

Fig. 4. FPGA Implementation – Hybrid Cryptographic Output (AES + ECC Combined)



The 7-segment display presents a hybrid encrypted output combining AES and ECC operations. The partial LED activation indicates a mid-stage pipeline state, where the AES substitution-permutation rounds are integrated with the ECC scalar multiplication output, demonstrating the seamless co-execution of both cipher families on the Artix-7 FPGA fabric.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:2 Volume No.10 March - April – 2026
DOI:10.46647/ijetms.2026.v10i02.046 ISSN: 2581-4621

Table 3.

Figure	Display Output	Represents
Fig.1	Pt6S	Random Key Generation
Fig.2	Ay22	ECC Key Output
Fig.3	Ct7F	AES Encryption + All LEDs
Fig.4	Dp6S	Hybrid AES+ECC Combined

V. CONCLUSION

This paper presented the design and FPGA realization of a hybrid cryptographic architecture integrating the Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and a hardware-based random key generation module on the Xilinx Artix-7 50T FPGA using the Nexys A7 development board. The proposed system successfully demonstrated the co-execution of two mathematically distinct cipher families within a unified reconfigurable hardware platform.

The hardware implementation confirmed that the AES module efficiently performed substitution-permutation rounds, while the ECC module executed scalar point multiplication over a prime field, both operating in a tightly coupled pipeline. The hardware-based random key generator ensured that cryptographic keys are generated with high entropy, eliminating the vulnerabilities associated with software-based pseudo-random number generators.

The 7-segment display outputs observed during hardware testing validated the correct functioning of each module — random key segments, ECC-derived key components, AES encrypted outputs, and the combined hybrid pipeline output — demonstrating reliable and repeatable operation on silicon.

The results confirm that FPGA-based hybrid cryptographic systems offer a compelling balance between the high throughput of symmetric encryption and the key exchange security of asymmetric cryptography. This architecture is well-suited for deployment in embedded security applications, IoT edge devices, and secure communication systems where both performance and security are critical constraints.

Future work will focus on extending the architecture to support higher key lengths, integrating a full key management protocol, and evaluating power consumption and timing performance using Xilinx Vivado implementation reports.

From a hardware efficiency perspective, the Xilinx Artix-7 50T FPGA proved to be a suitable and cost-effective platform for this implementation. The reconfigurable nature of the FPGA allowed rapid prototyping, iterative design refinement, and real-time hardware verification without the need for custom ASIC fabrication. The successful deployment on the Nexys A7 board demonstrates that

DOI:10.46647/ijetms.2026.v10i02.046 ISSN: 2581-4621

such hybrid cryptographic systems can be practically realized within the constraints of mid-range FPGA devices.

The proposed architecture holds significant potential for deployment in a wide range of security-sensitive applications including IoT edge devices, embedded medical systems, secure communication modules, and military-grade data protection systems where both computational performance and cryptographic strength are non-negotiable requirements.

Future work will focus on extending the architecture to support higher key lengths, integrating a full key management protocol, and evaluating power consumption and timing performance using Xilinx Vivado implementation reports

VI. REFERENCES

[1] J. Daemen and V. Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard," Springer-Verlag, Berlin, Germany, 2002.

[2] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, Jan. 1987.

[3] V. S. Miller, "Use of Elliptic Curves in Cryptography," in *Proc. CRYPTO 1985*, Lecture Notes in Computer Science, vol. 218, Springer, Berlin, pp. 417–426, 1986.

[4] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS Publication 197, Nov. 2001.

[5] National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)," FIPS Publication 186-4, Jul. 2013.

[6] Xilinx Inc., "Artix-7 FPGAs Data Sheet: DC and AC Switching Characteristics," DS181, Xilinx Product Documentation, 2018.

[7] Digilent Inc., "Nexys A7 Reference Manual," Digilent Technical Documentation, 2019. [Online]. Available: https://digilent.com/reference/programmable-logic/nexys-a7/reference-manual

[8] T. Güneysu and C. Paar, "Ultra High Performance ECC over NIST Primes on Commercial FPGAs," in *Proc. CHES 2008*, Lecture Notes in Computer Science, vol. 5154, Springer, Berlin, pp. 62–78, 2008.

[9] T. Good and M. Benaissa, "AES on FPGA from the Fastest to the Smallest," in *Proc. CHES 2005*, Lecture Notes in Computer Science, vol. 3659, Springer, Berlin, pp. 427–440, 2005.

[10] M. Hutter and E. Wenger, "Fast Multi-Precision Multiplication for Public-Key Cryptography on Embedded Microprocessors," in *Proc. CHES 2011*, Lecture Notes in Computer Science, vol. 6917, Springer, Berlin, pp. 459–474, 2011.

[11] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proc. CRYPTO 1999*, Lecture Notes in Computer Science, vol. 1666, Springer, Berlin, pp. 388–397, 1999.

[12] B. Sunar, W. J. Martin, and D. R. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks," *IEEE Transactions on Computers*, vol. 56, no. 1, pp. 109–119, Jan. 2007.

[13] S. B. Ors, F. Gürkaynak, E. Oswald, and B. Preneel, "Power-Analysis Attack on an ASIC AES Implementation," in *Proc. ITCC 2004*, IEEE, pp. 546–552, 2004.

[14] K. Sakiyama, L. Batina, B. Preneel, and I. Verbauwhede, "Multicore Curve-Based Cryptoprocessor with Reconfigurable Modular Arithmetic Logic Units over GF(2^n)," *IEEE Transactions on Computers*, vol. 56, no. 9, pp. 1269–1282, Sep. 2007.

[15] A. Satoh and K. Takano, "A Scalable Dual-Field Elliptic Curve Cryptographic Processor," *IEEE Transactions on Computers*, vol. 52, no. 4, pp. 449–460, Apr. 2003.