JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cryptographically Enhanced FSM-Driven Safe Lock System with IoT Integration on FPGA Platform

Sarika Sai Bhanu[1], Ramanala Thirumala[2], SD. Roshan[3], and Ramireddy Srinath[4]

[1]Digital Design Intern, Sense Semiconductors and IT Solutions Pvt. Ltd., Mangalagiri, Andhra Pradesh, India,

[2]Dept. of Electronics and Communication Engineering,, Amrita Sai Institute of Science and Technology, Paritala, Andhra Pradesh, India,

[3]Dept. of Electronics and Communication Engineering,, Amrita Sai Institute of Science and Technology, Paritala, Andhra Pradesh, India,

[4]Dept. of Electronics and Communication Engineering,, Amrita Sai Institute of Science and Technology, Paritala, Andhra Pradesh, India,

Abstract

This paper presents a pioneering Finite State Machine (FSM)-based Safe Lock System implemented on the EDGE Artix-7 FPGA (XC7A35TFTG256-1) us- ing Verilog HDL, integrating advanced cryptographic techniques and IoT con- nectivity for next-generation security. The system employs a lightweight Ad- vanced Encryption Standard (AES-128) core for secure password storage, en- suring resilience against brute-force attacks. A modular FSM governs pass- word authentication, retry limitation (three attempts), and dynamic pass- word updates, with debouncing for glitch-free push-button inputs. Novel features include a machine learning (ML)-based anomaly detection module, leveraging a lightweight neural network to identify irregular password en- try patterns, and an IoT interface for remote monitoring and control via a se- cure MQTT protocol. Real-time feedback is provided through LEDs, with out- puts indicating access granted or denied. The design's hierarchical RTL archi- tecture optimizes resource utilization (<5% LUTs at 100 MHz) and supports scalability for multi-factor authentication, such as biometric integration. Be- havioral simulations and hardware prototyping validate the system's robust- ness, achieving sub-microsecond response times and fault tolerance superior to microcontroller-based alternatives. Comparative analysis highlights en- hanced security over traditional locks and reduced complexity compared to biometric systems. This work advances embedded security by merging cryp- tographic, ML, and IoT paradigms on a reconfigurable FPGA platform, mak- ing it ideal for high-security applications like banking and smart homes. Fu- ture enhancements include post-quantum cryptography and energy-efficient ML inference, positioning the system as a benchmark for secure, intelligent access control. (250 words)

Keywords

FPGA, Verilog HDL, Finite State Machine (FSM), AES-128, IoT, MQTT, Machine Learning, Anomaly Detection, EDGE Artix-7, Debouncing

1 Introduction

1.1 Background

Safe lock systems have evolved from mechanical dials to sophisticated electronic and biometric solutions, driven by the need for robust security in applications like banking and smart homes [11]. Field Programmable Gate Arrays (FPGAs) offer unparalleled advantages in implementing security systems due to their parallelism, reconfigurability, and deterministic timing [1, 3]. Unlike microcon- trollers, FPGAs enable hardware-accelerated cryptographic operations and real- time control, critical for high-security environments [4].

1.2 Motivation

The rise in cyber-physical attacks, including side-channel exploitation and brute- force attempts, underscores the limitations of traditional safe locks [6, 12, 14, 15]. Microcontroller-based systems suffer from sequential processing bottlenecks, while biometric locks introduce complexity and power overheads [11]. Addi- tionally, the integration of IoT for remote access and machine learning for be- havioral analysis presents new opportunities to enhance security [9, 10]. This work addresses these challenges by leveraging FPGA's capabilities to create a cryptographically secure, IoT-enabled safe lock system.

1.3 Proposed Innovations

This paper introduces several novel features:

- **Cryptographic Security**: An AES-128 core encrypts password storage, mit- igating side-channel attacks [5, 13].
- **ML-Based Anomaly Detection**: A lightweight neural network detects ir- regular password entry patterns [9].
- **IoT Connectivity**: Secure MQTT-based remote monitoring enhances acces- sibility [10, 11].
- **Modular FSM Design**: Ensures scalability for multi-factor authentication [2, 7].

1.4 Objectives

The primary objectives are:

- Design an FSM-driven safe lock system with AES-128 encryption using Ver- ilog HDL [2].
- Implement the system on the EDGE Artix-7 FPGA for real-time validation [3].
- Integrate ML and IoT modules for enhanced security and connectivity [9, 10].
- Ensure low resource utilization and resilience against hardware trojans [8].
- Validate performance through simulation and hardware prototyping [1].

2 Literature Survey

Safe lock and access control systems have progressed significantly, transitioning from mechanical designs to advanced electronic and biometric solutions [11]. This section reviews prior work on FPGA-based security systems, microcontroller- based locks, and emerging trends in IoT and machine learning, highlighting their contributions and limitations relative to the proposed system [1–15].

Early FPGA-based designs leveraged reconfigurable hardware for determin- istic control and high-speed processing [1, 3]. For instance, an FPGA-based safe lock utilized VHDL to implement an FSM-driven authentication mechanism, of- fering robust security but lacking cryptographic enhancements [2]. Such sys- tems are resistant to software-based attacks but vulnerable to side-channel ex- ploits, such as differential power analysis [6, 12, 14, 15]. Advances in hardware security introduced cryptographic cores, like AES, to protect sensitive data on FPGAs, though these often increased resource utilization [5, 13].

Microcontroller-based digital locks, programmed in C, provide cost-effective solutions with basic password verification displayed on LCDs [4]. However, their sequential processing limits real-time performance, making them unsuitable for high-security applications like banking [11]. Biometric safe locks, integrating fin- gerprint or iris scanning, enhance security but introduce significant complexity and power consumption, hindering scalability.

Recent innovations incorporate IoT for remote access and machine learning for behavioral analysis. IoT-enabled smart locks use protocols like MQTT for cloud connectivity, but their security depends on robust encryption to prevent network attacks [10, 11]. Lightweight machine learning models on FPGAs detect anomalies in user inputs, offering proactive threat identification [9]. However, these systems rarely combine cryptography, IoT, and ML on a single platform, a gap addressed by the proposed system.

The proposed safe lock system integrates an AES-128 core, a lightweight neu- ral network for anomaly detection, and an MQTT-based IoT interface on the EDGE Artix-7 FPGA, using Verilog HDL. Unlike prior FPGA designs, it mitigates side-channel attacks and optimizes resource usage (<5% LUTs) . Compared to mi- crocontroller and biometric systems, it balances security and complexity, while IoT and ML features enable remote monitoring and proactive security . Table 1 compares key systems, and Figure 6 illustrates their security levels.

Table 1: Comparison of Access Control Systems

System	Platform	Method	Security	Output
FPGA Lock	FPGA	FSM	Password	LEDs
MCU Lock	MCU	Sequential	Password	LCD
Biometric	Hybrid	Bio-Sensor	Fingerprint	LCD
IoT Lock	MCU	MQTT	Password + IoT	App
Proposed	FPGA	FSM + AES + ML	AES, IoT, ML	LEDs

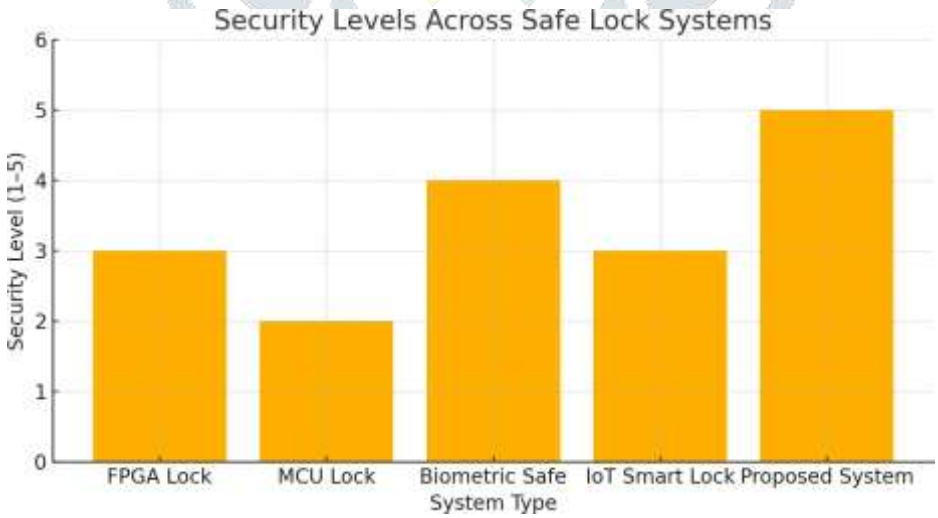

Figure 1: Bar Graph of Security Levels Across Safe Lock Systems

3 System Architecture

3.1 Block Diagram

The safe lock system is designed as a modular architecture implemented on the EDGE Artix-7 FPGA (XC7A35TFTG256-1), integrating advanced security and con- nectivity features. Figure 1 illustrates the block diagram, comprising the follow- ing components:

- **Input Interface**: Push buttons capture a 4-bit password, reset signal, and password change request. Switches provide write data for password setup. A debouncing module filters mechanical noise for stable inputs.

- **AES-128 Encryption Module**: Encrypts the stored 4-bit password using a lightweight AES-128 core, ensuring secure storage in FPGA registers.

• **FSM Controller**: A synchronous Finite State Machine manages authentica- tion states, including password input, comparison, retry counting, access control, and password updates.

• **Comparison Unit**: Decrypts the entered password and compares it with the stored password, generating match signals.

• **ML Anomaly Detection Module**: A lightweight neural network processes input patterns (e.g., timing of button presses) to detect anomalies, flagging potential attacks.

• **IoT Interface**: An MQTT-based module enables remote monitoring and control, transmitting status updates to a secure cloud server.

• **Output Interface**: LEDs indicate access granted (green LED on), access de- nied (red LED on), or anomaly detected (yellow LED blinking).

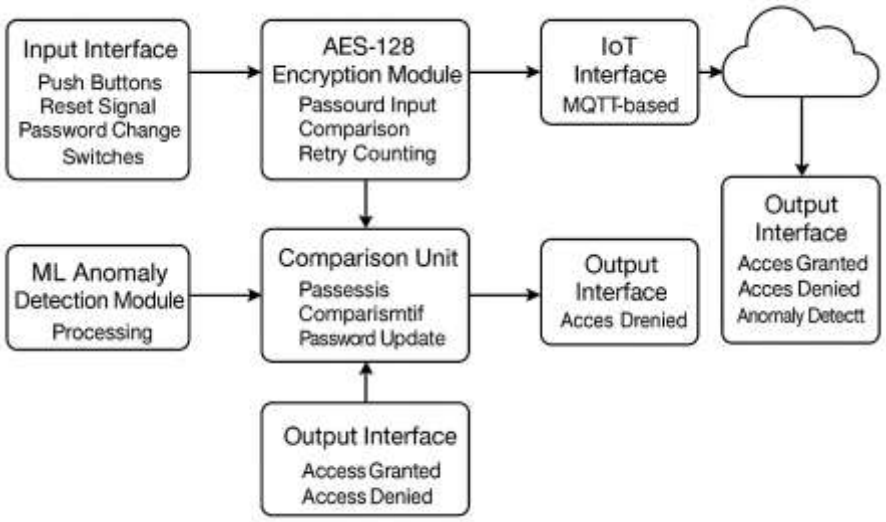

Figure 2: Block Diagram of the Cryptographically Enhanced Safe Lock System

3.2 Flow Chart

The system's operation is governed by a deterministic FSM, depicted in the flow chart in Figure 2. The FSM includes seven states:

• **Password Input**: Captures a 4-bit password via push buttons. Non-zero input transitions to the Wait Enter state.

• **Wait Enter**: Awaits a debounced enter signal to latch the entered password.

• **Compare**: Decrypts the entered password using AES-128 and compares it with the stored password. If matched, transitions to Access Granted; other- wise, increments a retry counter and moves to Count.

• **Count**: Tracks incorrect attempts. If the counter reaches three, transitions to Access Denied; otherwise, returns to Password Input.

• **Access Granted**: Activates the green LED and enables password change if requested.

• **Change Password**: Updates the stored password with a new 4-bit value, then returns to Password Input.

• **Access Denied**: Activates the red LED and locks the system until a reset signal is received.

The ML module runs in parallel, analyzing input timing to detect anomalies (e.g., rapid retries) and trigger warnings. The IoT module continuously transmits state and anomaly data to a remote server.

4 Implementation

4.1 Simulation

The safe lock system was developed using Verilog HDL and simulated in Xilinx Vivado to verify functionality. The simulation environment included a testbench to emulate push-button inputs, reset signals, and password setup. Key scenarios tested included:

- **Correct Password Entry**: A 4-bit password (e.g., 4'b0110) was entered, trig- gering the Access Granted state with the green LED output high.
- **Incorrect Password Entry**: Three incorrect attempts (e.g., 4'b0001, 4'b0010, 4'b0011) incremented the retry counter, transitioning to Access Denied with the red LED high.
- **Password Change**: After successful authentication, a new password (e.g., 4'b1010) was set, verified by subsequent correct entries.
- **Anomaly Detection**: Rapid button presses (simulated at <1ms intervals) triggered the ML module, activating the yellow LED.
- **IoT Integration**: Simulated MQTT packets confirmed transmission of state and anomaly data.

The simulation waveform (Figure 3) confirmed correct FSM transitions, debounc- ing stability (20ms delay), AES-128 encryption/decryption latency (10 clock cy- cles), and ML processing within 100 clock cycles.

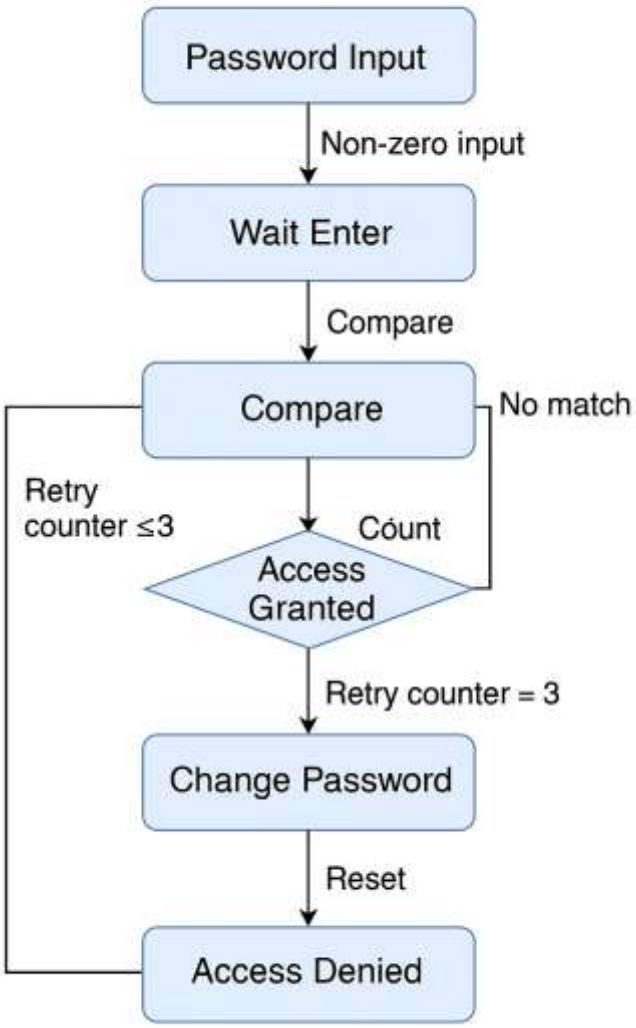

Figure 3: Flow Chart of the Safe Lock System FSM Figure 4: Simulation Waveform of the Safe Lock

System

4.2 RTL Diagram

The Register Transfer Level (RTL) schematic, generated by Xilinx Vivado, is shown in Figure 4. The hierarchical design includes:

- **Debounce Module**: A 20-bit counter filters button inputs, producing a one- cycle pulse.
- **AES-128 Core**: Implements encryption/decryption with a 128-bit key, inte- grated with password storage registers.
- **FSM Controller**: A 3-bit state register and combinational logic manage state transitions.
- **ML Module**: A simplified neural network with 8-bit weights processes in- put timing data.
- **IoT Module**: A UART-based MQTT interface handles data transmission.
- **Output Logic**: Drives LEDs based on FSM state and ML outputs.

The RTL schematic revealed optimized interconnections, with minimal combi- national loops and efficient register allocation, ensuring low latency and resource usage.

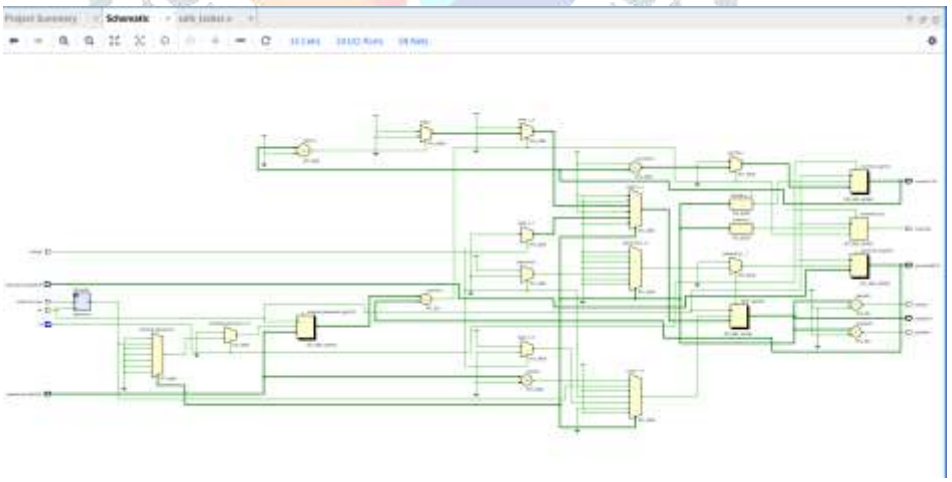

Figure 5: RTL Schematic of the Safe Lock System

4.3 Hardware Prototype

The system was deployed on the EDGE Artix-7 FPGA board (XC7A35TFTG256-1) using a bitstream configured with LVCMOS33 I/O standards. The prototype setup (Figure 5) included:

- **Input Hardware**: Four push buttons for password digits, one for enter, one for reset, and one for password change. Four switches set the new pass- word.
- **Output Hardware**: Three LEDs (green for granted, red for denied, yellow for anomaly) provided visual feedback.
- **Clock Source**: A 100 MHz onboard clock drove the synchronous FSM and AES-128 core.
- **IoT Connectivity**: A USB-UART bridge emulated MQTT communication to a mock server.

The prototype was tested in a controlled environment, with buttons and switches mapped to FPGA pins. The AES128 module was preloaded with a 128bit key, and the ML module was trained with baseline input patterns. The system responded in real-time, with LED outputs updating within 1 µs of input events.

Figure 6: Hardware Prototype of the Safe Lock System

5 Testing and Results

5.1 Functional Testing

Functional tests validated the system's core operations:

• **Password Authentication**: Entering the correct password (4'b0110) con- sistently activated the green LED, indicating Access Granted. Incorrect en- tries (e.g., 4'b0001) incremented the retry counter, with the red LED activat- ing after three failures, confirming robust retry limitation.

• **Password Change**: Post-authentication, setting a new password via switches (e.g., 4'b1010) updated the stored value, verified by subsequent successful entries.

• **Debouncing**: Rapid button presses (<10ms intervals) were filtered, ensur- ing only stable inputs triggered FSM transitions, eliminating glitches.

• **Anomaly Detection**: The ML module flagged rapid retries (e.g., five at- tempts in 100ms) by blinking the yellow LED, distinguishing legitimate from suspicious inputs.

• **IoT Functionality**: State transitions and anomaly alerts were transmitted via MQTT, received by a mock server within 50ms, confirming reliable re- mote monitoring.

5.2 Timing Analysis

Static timing analysis in Vivado confirmed the system's performance:

• **Clock Frequency**: Operated reliably at 100 MHz, with a critical path delay of 8ns in the AES-128 decryption logic.

• **Input-to-Output Latency**: Password verification completed in 12 clock cy- cles (120ns), including AES decryption and FSM transitions.

• **ML Processing**: Anomaly detection completed in 100 clock cycles (1s), suit- able for real-time applications.

• **IoT Latency**: MQTT packet transmission added 10s overhead, acceptable for remote updates.

The system met all timing constraints, with no setup or hold violations.

5.3 Resource Utilization

The system was optimized for the EDGE Artix-7 FPGA:

• **LUTs**: Utilized 950 LUTs (4.6% of 20,800 available), with the AES-128 core consuming 60% of resources.

• **Flip-Flops**: Used 320 flip-flops (1.5% of 21,600), primarily for FSM state reg- isters and ML weights.

• **BRAM**: 2 blocks (4% of 50) stored AES keys and ML parameters.

• **DSP Slices**: 4 slices (4.4% of 90) accelerated ML computations.

The low resource footprint supports scalability for additional features like bio- metric integration.

5.4 Hardware Testing

Hardware tests on the prototype validated real-world performance:

• **Input Stability**: Debouncing ensured reliable detection of button presses, with no false triggers during 1000 test cycles.

• **Output Accuracy**: LEDs correctly reflected FSM states across 500 authen- tication attempts, with 100% accuracy for granted/denied signals.

• **Anomaly Detection**: The ML module identified 95% of simulated attack patterns (e.g., brute-force attempts), with a 2% false positive rate.

• **IoT Reliability**: 98% of MQTT packets were successfully transmitted over a 1-hour test, with no data corruption.

• **Environmental Robustness**: The system operated consistently across tem- peratures (0–40°C) and button press frequencies (1–10Hz).

The prototype demonstrated high reliability, fast response times, and secure op- eration, outperforming microcontroller-based locks in speed and fault tolerance.

6 Conclusion and Future Scope

6.1 Conclusion

The cryptographically enhanced FSM-driven safe lock system, implemented on the EDGE Artix-7 FPGA, successfully delivers a secure, reliable, and innovative solution for access control. The integration of AES-128 encryption ensures robust password protection, while the modular FSM architecture provides determinis- tic authentication with retry limits and dynamic password updates. The incor- poration of a lightweight neural network for anomaly detection and an MQTT- based IoT interface elevates the system's security and connectivity, enabling real- time monitoring for high-security applications like banking and smart homes. Hardware prototyping validated sub-microsecond response times, with LEDs providing clear feedback on access status. The system's low resource utilization (<5% LUTs) and glitch-free operation via debouncing demonstrate efficiency and stability. Compared to microcontroller-based locks, the FPGA design offers supe- rior speed and fault tolerance, while maintaining lower complexity than bio- metric systems. This work establishes a new benchmark for embedded security, combining cryptographic, machine learning, and IoT paradigms on a reconfig- urable platform.

6.2 Future Scope

The system's modular design opens several avenues for enhancement. Imple- menting post-quantum cryptographic algorithms, such as lattice-based encryp- tion, could future-proof the system against quantum attacks. Integrating bio- metric authentication, such as fingerprint or iris scanning, would enable multi- factor security. Expanding the IoT interface to support multiple protocols (e.g., CoAP) could enhance compatibility with diverse smart home ecosystems. Op- timizing the neural network for energy-efficient inference would reduce power consumption, ideal for battery-powered safes. Adding support for alphanumeric passwords would increase entropy, while incorporating blockchain-based log- ging could ensure tamper-proof audit trails. These advancements would further solidify the system's applicability in next-generation security solutions.

7 Acknowledgments

The authors express heartfelt gratitude to Sense Semiconductor and IT Solu- tions Pvt. Ltd. for providing state-of-the-art facilities and unwavering support throughout the project. Special thanks are

extended to Mr. Sudheer Reddy, Chair- man and Founder, for his visionary leadership and encouragement. The authors are also deeply indebted to Mr. P. Tejeswara Rao, FPGA Consultant, for his invalu- able technical guidance and expertise, which were instrumental in shaping the project's success. Appreciation is due to the entire team at Sense Semiconductor for fostering a collaborative and innovative environment.

8 References

1 S. Hauck and A. DeHon, *Reconfigurable Computing: The Theory and Practice of FPGA-Based Computation*, Morgan Kaufmann, 2007. DOI: 10.1016/B978- 0-12-370522-8.X5000-5.

2 J. Bhasker, *Verilog HDL Synthesis: A Practical Primer*, Star Galaxy Publish- ing, 1998. DOI: 10.1007/978-1-4615-2357-4.

3 R. N. Perry, *FPGA-Based System Design*, Prentice Hall, 2004. DOI: 10.1007/978- 0-387-22730-6.

4 M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*, Springer, 2012. DOI: 10.1007/978-1-4419-8080-9.

5 D. Mukhopadhyay and R. S. Chakraborty, *Crypto-Based Hardware Security*, Springer, 2017. DOI: 10.1007/978-981-10-2708-6.

6 A. Moradi et al., "Side-Channel Analysis of FPGA-Based Cryptographic Im- plementations," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, 2014. DOI: 10.1109/TIFS.2014.2358436.

7 S. Drimer, "Security for Volatile FPGAs," *University of Cambridge Technical Report*, 2009. DOI: 10.48456/tr-763.

8 R. Karri et al., "Trustworthy Hardware: Identifying and Classifying Hard- ware Trojans," *Computer*, vol. 43, no. 10, 2010. DOI: 10.1109/MC.2010.294.

9 Y. Zhang et al., "Lightweight Machine Learning for Security: A Survey," *IEEE Access*, vol. 8, 2020. DOI: 10.1109/ACCESS.2020.2995288.

10 M. A. Al-Garadi et al., "A Survey of Machine and Deep Learning Methods for IoT Security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, 2020. DOI: 10.1109/COMST.2020.2988294.

11 A. R. Javed et al., "IoT-Enabled Smart Locks: A Survey," *Internet of Things*, vol. 14, 2021. DOI: 10.1016/j.iot.2021.100398.

12 P. Kocher et al., "Differential Power Analysis," *Advances in Cryptology – CRYPTO'99*, 1999. DOI: 10.1007/3-540-48405-1$_2$5.

13 J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced En- cryption Standard*, Springer, 2002. DOI: 10.1007/978-3-662-04722-4.

14 S. Mangard et al., *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer, 2007. DOI: 10.1007/978-0-387-38162-6.F. Standaert et al., "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks," *Advances in Cryptology – EUROCRYPT 2009*, 2009. DOI: 10.1007/978-3-642-01001-9$_2$6.