ROAD TO 45 YEARS BINUS CO-CREATING THE INTELLIGENT SOCIETY

BINUS UNIVERSITY DOCTORATE PROGRAM

Doctor of Computer Science

Promovendus
Andi Sama
(2540136324)

Promotor
Prof. Dr. Ir. Meyliana, S.Kom., M.M., IPU, CDMS, CBDMP, CME

Co-Promotor 1
Dr. Ir. Yaya Heryadi, M.Sc.

Co-Promotor 2
Ir. Taufik, S.T., M.M., Ph.D., IPM

Lightweight Advanced Encryption Standard (AES) Model to Secure Data Transfer in Industrial Control Systems for Smart Factory in Manufacturing Industry

Background

- ✓ Security threats in OT systems are a recent trend in ICS, Industrial Control Systems (Stouffer et al., 2023; Jayalaxmi et al., 2021).
- ✓ The IT/OT convergence introduces security risks to OT systems (Cyber attack), including PLCs, the core controller in ICS (Wu H, Geng Y, Liu K, Liu W., 2019)
- ✓ Lack of encryption in industrial protocols. A secure communication between IoT devices to protect the data is essential [Jayalaxmi, P. et al. (2021)]
- ✓ PLC has been the core automation in Industrial Automation and the manufacturing industry since the beginning of Industry 3.0 (Yadav R, Namekar S., 2020)
- ✓ Symmetric scheme is computationally inexpensive compared to the Asymmetric [Maqsood, F. *et al.* (2017)], suitable for ICS (low resource requirements).
- ✓ In 2000, NIST announced the selection of the Rijndael block cipher family for the AES for Symmetric Encryption [Morris J. Dworkin, 2023]
- ✓ For the security aspect and implementation complexity, AES is considered as one of the strongest and most efficient algorithms [John, S. k (2023)]
- ✓ Modifying the existing algorithm: AES for lightweight applications is possible [John, S. k (2023)]
- ✓ The Lightweight AES (LAES) algorithm increased higher than AES by 4.2969% in terms of avalanche effect, meaning increased security [Salman, R.S., Farhan, A.K. and Shakir, A. (2022); Acla, H.B., and Gerardo, B.D. (2019)]

In Industrial Control Systems (ICS) within Industry 4.0, lightweight cryptography (LWC) is crucial for securing the Internet of Things (IoT)/Industrial IoT (IIoT). IoT devices have limited resources (memory, CPU, and battery) and thus require light techniques for securing communications. LWC is a collection of solutions for encryption techniques that feature devices with low computational complexity. It aims to expand the applications of cryptography to limited-resource devices while providing a high level of security (Mammeri, 2024, p. 194).

Research Objectives

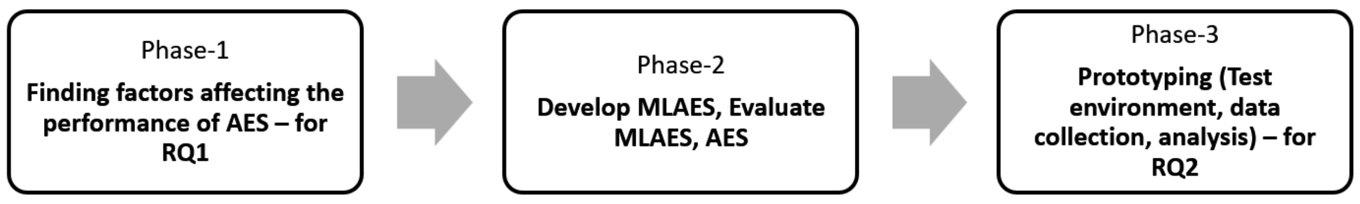
Securing data exchange in ICS through the modification of the symmetric-based encryption algorithm, based on the AES, Advanced Encryption Standard, for lightweight applications.

Methodology

- Action research: Systematically looks at the problem and tries various solutions.
- Quantitative: comparative (execution times) between MLAES (Modified Lightweight AES) and AES

Research Methodology

Approach: Quantitative: comparative (execution times) between MLAES (Modified Lightweight AES) and AES.
Justification: Apply the software reengineering framework to obtain a faster modified AES algorithm for lightweight applications.
1. Reverse Engineering: understand how the algorithm works. 2. Restructuring: make modifications to obtain better execution time (develop, evaluate). 3. Forward Engineering: do the prototyping and measure the execution time of MLAES encrypt/decrypt (test and evaluate)



Phase-1
Finding factors affecting the performance of AES – for RQ1

Phase-2
Develop MLAES, Evaluate MLAES, AES

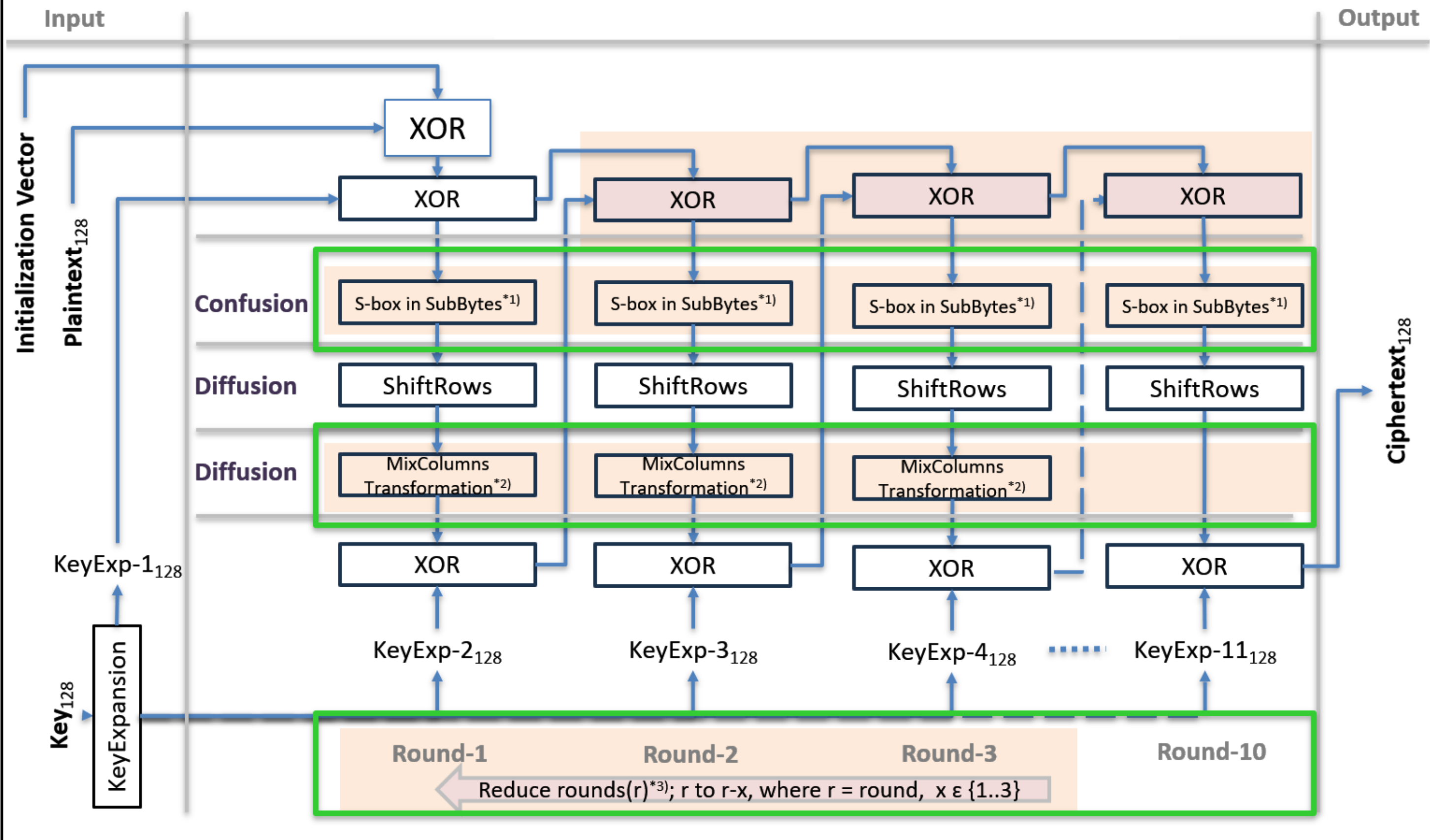
Phase-3
Prototyping (Test environment, data collection, analysis) – for RQ2

- ✓ Dataset/acquisition
  - ➢ Search: Google, multiple index databases
  - ➢ Retrieval: Google Scholar, Research Gate, Binus LKC, others
- ✓ Sampling (article selections): PRISMA framework for SLR
- ✓ Data analysis: PRISMA framework for SLR
- ✓ Tools: Reference Manager: Mendeley

- ✓ Dataset/acquisition: SoTA paper, JSON (synthetic),
- ✓ Data analysis/measurement metrics: SPSS (Mann-Whitney)/ hamming distance
- ✓ Tools:
  - ➢ OS: Windows; Programming Language: C
  - ➢ Compiler: gcc.; Editor: Notepad+

- ✓ Dataset/acquisition: SoTA paper (20 data points), algorithm execution times from prototyping
- ✓ Sampling (execution times): encrypt, decrypt operation for MLAES, AES algorithms; 600 data points = 30 x SoTA dataset (each for MLAES encrypt/decrypt and AES encrypt/decrypt)
- ✓ Data analysis/measurement metrics: SPSS (t-test)/p-value for mean difference of execution times MLAES, AES
- ✓ Tools:
  - ➢ OS: Windows; Programming Language: C
  - ➢ PLC: Siemens, BOSCH Rexroth; Gateway: Node-RED; Visualization (SCADA): SCADABR
  - ➢ Network trace tools: Wireshark
  - ➢ Measurement metrics: p-value at significance level
  - ➢ Validating Prototyping Environment: FGD with Subject Matter Expert

Model, MLAES – Modified AES for Lightweight Applications



*1)S-box in SubBytes: modify S-box table; *2)MixColumns transformation: modify transformation matrix; *3) 10 to 8

Conclusion

MLAES algorithm, is based on the AES with the purpose to obtain an improved version that runs faster while utilizing fewer resources while providing secure data exchange within ICS environment. MLAES enables a more efficient and secure data exchange among connected systems in ICS by embedding security, making them less vulnerable to cyber attacks in Industry 4.0. In terms of execution time performance during prototyping, MLAES is faster than AES (statistically significant), while maintaining the same level of security performance.

Benefits/Implications

A better result, on average, in terms of avalanche effect, although statistically insignificant, indicates a qualitatively better security. MLAES provides lightweight security to improve computation time (faster execution) for low-resource devices such as IoT within ICS in the Manufacturing Industry or Industrial Automation in general. MLAES will provide less latency in an FPGA-based hardware implementation compared to a software implementation, such as PLC firmware or a Node-RED application, in an edge computing gateway.

Limitations

MLAES, based on AES-128 is limited to 128-bit (key size). Prototyping is on local network. However, it is expected that the execution times of MLAES/AES encryption/decryption will be similar to the actual PLC, e.g., with JSON dataset.

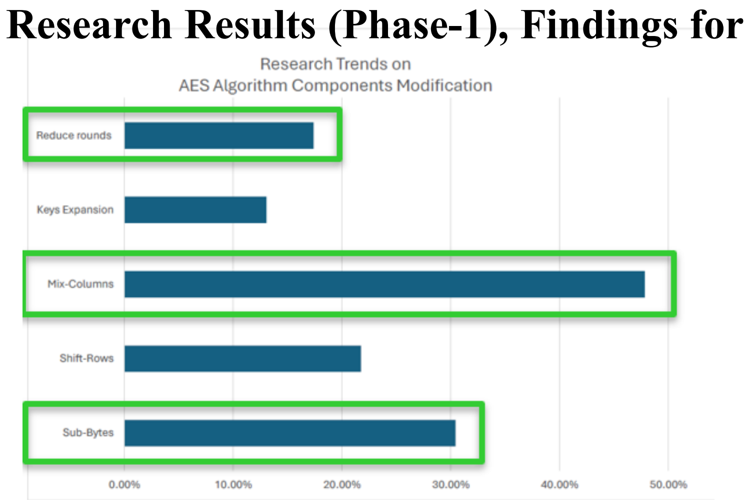
Suggestion/Future Work

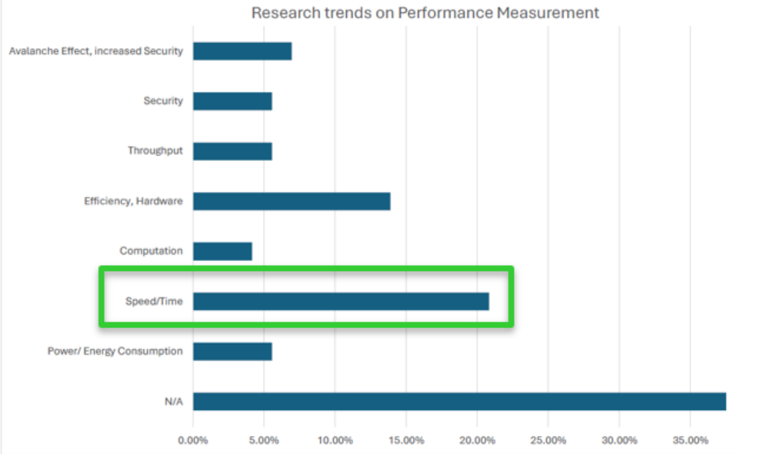
Future theoretical contributions could enhance the algorithm by further exploring the transformation into an S-box table within the SubBytes operation, modifying the ShiftRows and MixColumns algorithms, and considering the use of lightweight computing power and limited resources in embedded systems.
Future practical implementation research may involve implementing the MLAES on PLCs within the firmware or FPGA; or within PLCs that support Node-RED, edge computing, or IoT devices within ICS.

Research Questions

RQ-1: What factors that affect the performance of the lightweight Advanced Encryption Standard (AES) algorithm?
RQ-2: How to obtain an improved version of the AES algorithm that runs faster but utilizes fewer resources?

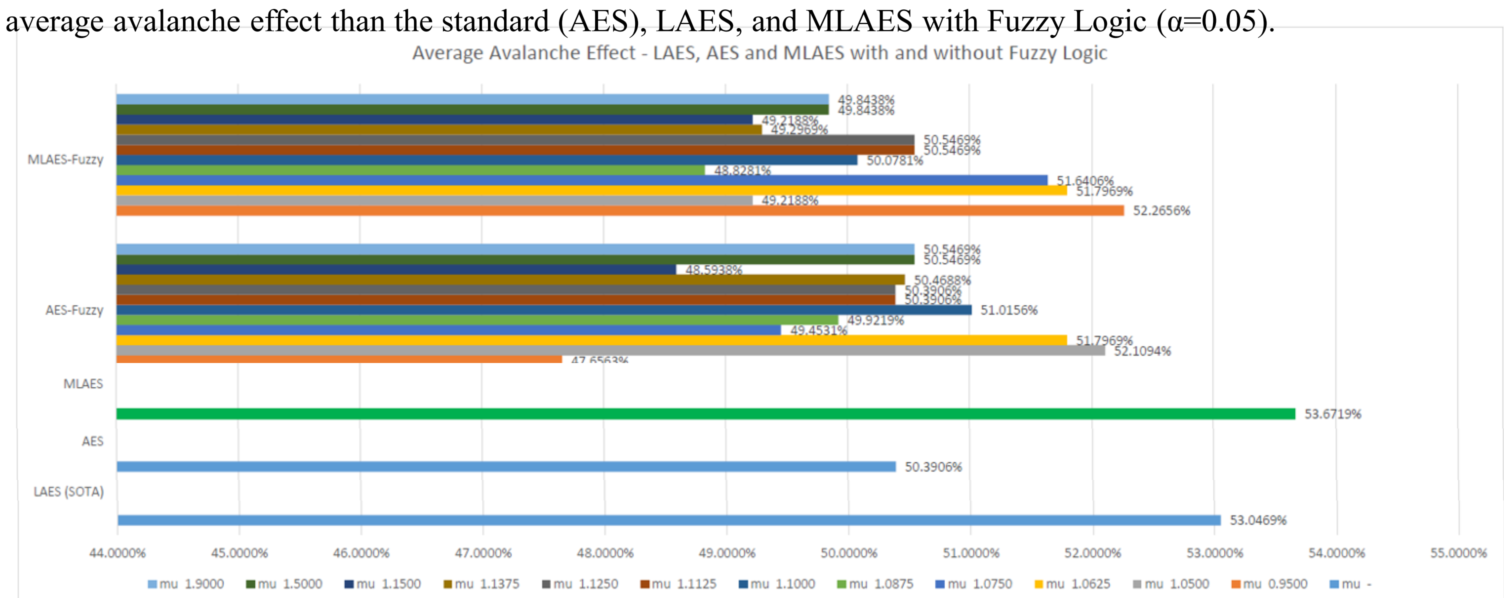
Research Results (Phase-1), Findings for RQ1



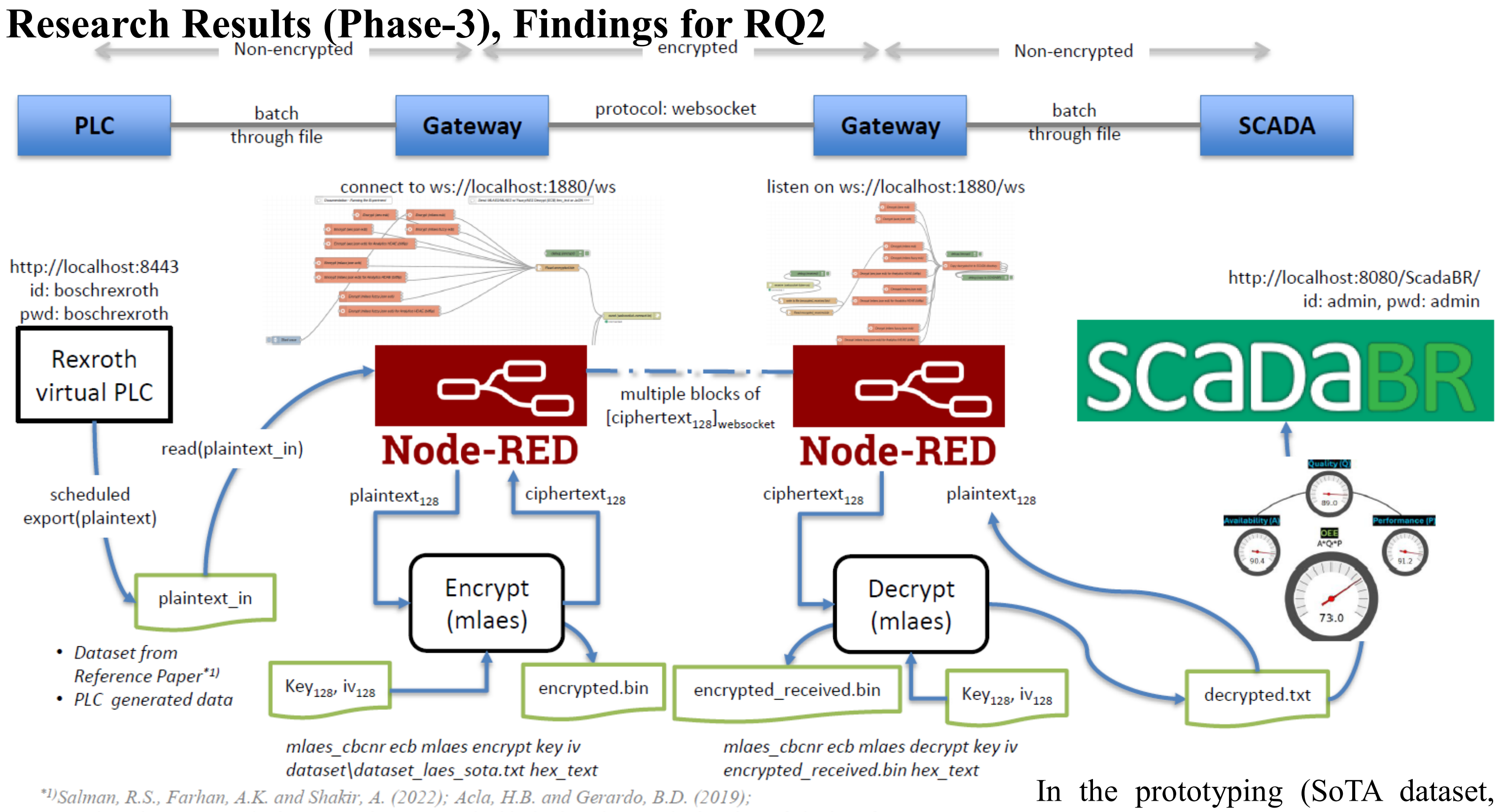


Research Results (Phase-2), Experiments

With SoTA (state-of-the-art) dataset from the reference paper (Acla and Gerardo, 2019; Salman, Farhan, and Shakir, 2022), the Modified Lightweight AES (MLAES) achieved **53.6719%** in average avalanche effect. MLAES is **1.5625%**, **1.4063%**, and **0.6250%** higher than AES with fuzzy logic (**52.1094**%, μ=1.0500), MLAES with fuzzy logic (52.2656%, μ=0.9500), and the SoTA Lightweight AES, LAES (**53.0469%**)—fuzzy logic with a tent chaotic map inference rule and a center-of-gravity method for defuzzification. Despite insignificant statistical performance improvement (fivefold dataset, SoTA+) with the Mann-Whitney statistical test, MLAES has qualitatively better average avalanche effect than the standard (AES), LAES, and MLAES with Fuzzy Logic (α=0.05).



Research Results (Phase-3), Findings for RQ2

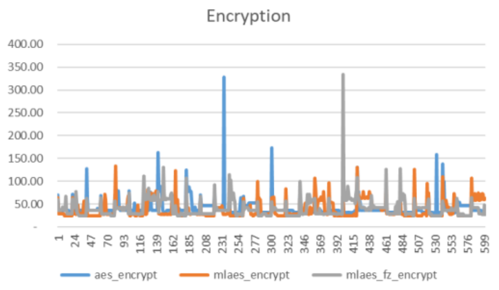


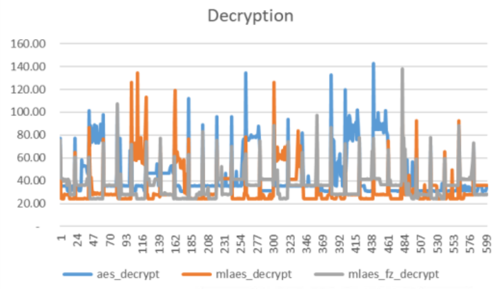
- Dataset from Reference Paper*1)
- PLC generated data

mlaes_cbcnr ecb mlaes encrypt key iv dataset\dataset_laes_sota.txt hex_text

mlaes_cbcnr ecb mlaes decrypt key iv encrypted_received.bin hex_text

*1)Salman, R.S., Farhan, A.K. and Shakir, A. (2022); Acla, H.B. and Gerardo, B.D. (2019);
Key, iv (initialization vector), plaintext, ciphertext: 128-bit block; algorithm: aes | mlaes | aes_fz | mlaes_fz





In the prototyping (SoTA dataset, N=600 for each algorithm (MLAES, AES) and mode of operations (encrypt, decrypt), α=0.01), there is a **statistically significant mean difference** in the **execution time** for the **encryption** and **decryption operations** between the **MLAES** and **AES** algorithms, validated by t-test statistics for two independent samples.

In terms of execution time, MLAES is faster than AES, by utilizing fewer resources (decreasing the original AES rounds from 10 to 8).

Publications

- Conference, Procedia Computer Science, 2023, Indexed, Acquiring Automation and Control Data in The Manufacturing Industry: A Systematic Review (citation: 4)
- Conference, ICICyTA, 2023, Indexed, Implementation of Lightweight PRNG on PLC for Industrial Control Systems
- Conference for RSCH9016 Publication I (ICCTech, 2024, Indexed), Random Number Generator for Securing Data Exchange in Smart Factory - Recent Trends and Best Practices
- Journal for RSCH9018 Publication II (IJSSE, 2024, Indexed), Lightweight Pseudo Random Number Generator for Embedded Systems
- Journal for RSCH9020 Publication III (IJSSE, 2025, Indexed), Modified Lightweight Advanced Encryption Standard for Lightweight Applications