ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

ĐÀO MẠNH HIỆP

NGHIÊN CỨU THIẾT KẾ BẢO MẬT THẺ RFID SỬ DỤNG MÃ HÓA ĐƯỜNG CONG ELLIPTIC

(Secure Lightweight RFID tag with Elliptic Curve Cryptography)

Ngành đào tạo: Kỹ thuật Điện tử
Mã số: 9520203

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT ĐIỆN TỬ

HÀ NỘI – 2025

Công trình được hoàn thành tại: Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội

Người hướng dẫn khoa học:

1. GS. TS Trần Xuân Tú
2. GS. TS Vincent Beroulle

Phản biện:.....

.....

Phản biện:.....

.....

Phản biện:.....

.....

Luận án sẽ được bảo vệ trước Hội đồng cấp Đại học Quốc gia chấm luận án tiến sĩ họp tại .....

vào hồi….. giờ…..ngày…..tháng…..năm……

Có thể tìm hiểu luận án tại:

- Thư viện Quốc gia Việt Nam
- Trung tâm Thông tin - Thư viện, Đại học Quốc gia Hà Nội

Introduction

Radio Frequency Identification (RFID) has been a breakthrough in wireless authentication technology in several applications, ranging from the military to civil devices. In the general RFID system, there are two main parties: tags and a reader for authentication. Depending on the particular application, the tags could utilize the internal battery (active RFID tags) or energy harvesting (passive RFID tags). Reducing the internal battery helps the device become smaller and cheaper. As a result, passive RFID tags significantly contribute to the development of hand-held applications such as e-passports, civil cards, and contactless payment cards.

Although playing a critical role in several applications, especially security authentication devices, passive RFID tags face several vulnerabilities, including wireless and hardware attacks. To mitigate these threats, integrating embedded cryptography, such as Elliptic Curve Cryptography (ECC), into the passive RFID tags is critical to protect the data. However, deploying ECC on passive RFID tags presents significant challenges, as listed below:

1. **Physical resource limitations:** Passive RFID tags face strict restrictions in power consumption, area cost, and latency. As the passive RFID tag harvests energy from the electromagnetic field over the rectifier antenna (rectenna), its operational power is limited by the efficiency of energy conversion. Besides, the communication time between the tag and the reader is quite short and standardized, which caps interaction time at 20 milliseconds, according to the ISO/IEC-14443, severely restricting available energy. Therefore, the harvested energy of the tag is significantly constrained. Additionally, minimizing the design's physical footprint is critical to reducing manufacturing expenses.

2. **Security requirements:** Protection approaches for the passive RFID tags to be robust against wireless and hardware attacks present a complementary complexity in processing. In particular, at the protocol layer, addressing the wireless attacks, countermeasures for ECC-based authentication protocols tend to implement

additional security primitives, such as random generators, hash functions, and supplementary scalar multiplication steps. Consequently, the implementation costs of the system dramatically increase. Regarding hardware challenges, hiding or masking techniques are designed to prevent side-channel attacks. These techniques require additional computations during processing to minimize the leakage of the secret key through side channels, which enlarges the implementation costs of the device.

Besides, employing the ECC-based authentication protocol is processed over multiple design layers, from the protocol to the security primitives; there is a wide range of choices, such as communication schemes, algorithms, or architectures in each layer. Therefore, the design space of the ECC-based authentication protocol is complicated for designers to explore. Besides, there are issues of multi-object optimization in a wide design space, as the ECC-based authentication protocol raises the time-to-market, which also impacts production expenses.

This thesis proposes an effective hardware design and an innovative design methodology to address these problems. The dissertation covers the following key contributions:

1. As an initial step, we proposed a low-cost, low-power Elliptic Curve Cryptography named Binary Edwards Curve (BEC), targeting the passive RFID tags by utilizing the conventional Top-down design methodology.

2. To address the issue of time-to-market, an innovative Early Evaluation Meet-in-the-Middle (EEMitM) design methodology is proposed. The goal of this proposal is to provide a framework that helps designers quickly choose the most compatible design that meets multiple objectives of the constraints. To further develop the proposed EEMitM mentioned above, early estimation and evaluation approaches are proposed. This proposal enables designers to estimate the hardware implementation cost and security level of the databases early, without implementing on hardware. In addition, this work also permits designers to evaluate distinguished design solutions to choose the most compatible design.

Chapter 1
RFID System and Security Issues

This chapter presents the general concepts of the RFID system and its challenges. The main objective of the research is to employ ECC-based RFID tags in hardware implementation. The existing solutions for ECC-based authentication of RFID tags have also been reviewed. By assessing these solutions in the literature, this chapter shows the gap in the hardware implementation of the ECC-based passive RFID tags. Besides, it is necessary to find an optimal hardware design for ECC-based passive RFID tags that balances minimizing implementation costs and enhancing the security level.

1.1 General Concept of Secured Passive RFID System

1.1.1 Authentication System by Radio Frequency

A systematic concept of secured radio frequency authentication is presented in this section. The main components of the radio frequency authentication system are also reviewed in Figure 1.1 before an illustration of the authentication process between tags and the reader.

1.1.2 Radio Frequency Identification Tags

This section defines a classification of the Radio Frequency Identification System based on the structure of the tags. The benefits and drawbacks of these types of RFID tags are also highlighted to highlight the advantages of passive RFID tags in deploying constrained applications, such as retail stock management or contactless payment cards. Driven by these advantages, the global RFID market is expected to develop rapidly in the following decades.

1.2 Challenges of the Passive RFID Tags

1.2.1 Limitation of physical implementation costs

Although the RFID system has developed significantly based on its benefits, it also has several drawbacks. This section provides a brief overview of passive RFID tags in terms of implementation costs, such as latency and power consumption.

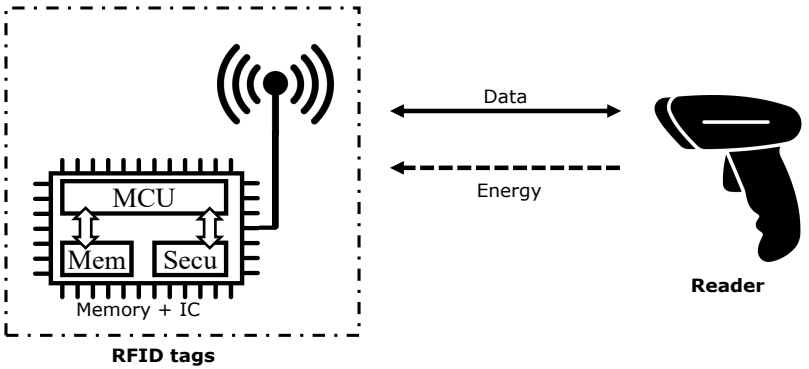


Figure 1.1: General Authentication System by Radio Frequency

1.2.2 Security Challenges for Passive RFID Tags

As passive RFID tags are used to communicate via the wireless channel, they are also threatened by various vulnerabilities. This section introduces the security challenges for passive RFID tags in terms of wireless and hardware attacks. Generally, these vulnerabilities utilize the weak points in the authentication algorithm or cryptographic mechanism to break the security characteristics.

1.3 Security Strategies for Passive RFID Tags

1.3.1 Authentication and Identification Protocols

Several countermeasures for passive RFID Tags are implemented in alternative levels of the system, ranging from authentication protocols to security hardware primitives to protect user data. This section briefly introduces the use of authentication protocols in passive RFID applications. Additionally, the characteristics and implementation cost of the authentication protocol are also mentioned.

1.3.2 Cryptography Primitives

In another level of countermeasures implementation, the cryptography primitive is carried out to encrypt the data using the secret key. This processing ensures the integrity of the system. Among encryption mechanisms, asymmetric encryption, such as Elliptic Curve Cryptography (ECC), is proposed to replace the symmetric approaches due to the benefits of the Discrete Logarithm Problem.

While ECC offers advantages in computational throughput and power efficiency compared to the other asymmetric algorithms in hardware implementation, it struggles to meet the implementation cost and energy constraints of devices, especially passive RFID tags. However, it is a challenge for researchers to look for optimal hardware-based passive RFID tags that balance the security level and the implementation costs.

Conclusion

This thesis chapter presents a systematic overview of the RFID System and its critical challenges. The main objective of the research is to deploy the ECC-based authentication protocol in hardware that balances the physical constraints with security-level requirements.

As the design space of ECC-based authentication protocols is exceptionally huge, it is a challenge for designers to find optimal architectures that balance both the security level and physical constraints. Conventional design methodologies enable designers to consider a systematic security evaluation only after the design phase. This limitation often necessitates costly countermeasures.

Addressing this limitation of traditional design approaches, this thesis proposes a novel framework that integrates security-implementation cost evaluation at early stages in the development cycle of ECC-based passive RFID systems.

Chapter 2

Design Methodology for Secured RFID Tags

This section reviews the existing design methodology for secured hardware implementation and the emerging AI-driven approaches.

2.1 Background and Motivation

2.1.1 Definition of Design Methodology

Firstly, this section defines the Electrical System Level (ESL) to model and analyze complicated systems based on their functionality and architecture. The ESL of the RFID system includes four layers, as depicted in Figure 2.1. The ESL of the RFID system initializes the Design Space Exploration for the design to identify and assess various design alternatives to optimize the hardware system. By utilizing the design methodology, the designers are provided several key benefits as follows:

- **Fast Prototyping**
- **Optimization**
- **System Integration**

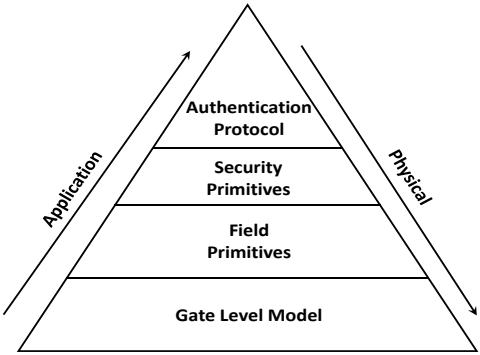


Figure 2.1: Pyramid of the implementation level of ECC-based authentication device.

2.1.2 Motivation of Research

By analyzing both the general design methodologies for hardware implementation and the secure design process, we determined the limitations that raise the design time of the final products. As the DSE becomes more complicated, the number of trial-and-error instances of designing increases significantly. As a result, the time-to-product cost rises in proportion.

By realizing the gap, this thesis proposes a novel design methodology that integrates both the security evaluation and the estimation of the implementation cost into the DSE loop. To demonstrate the improvements by utilizing the proposed design methodology, firstly, in this chapter, a detailed analysis of the conventional design methodologies for hardware implementations and an overview of the emerging AI-based design approaches are discussed.

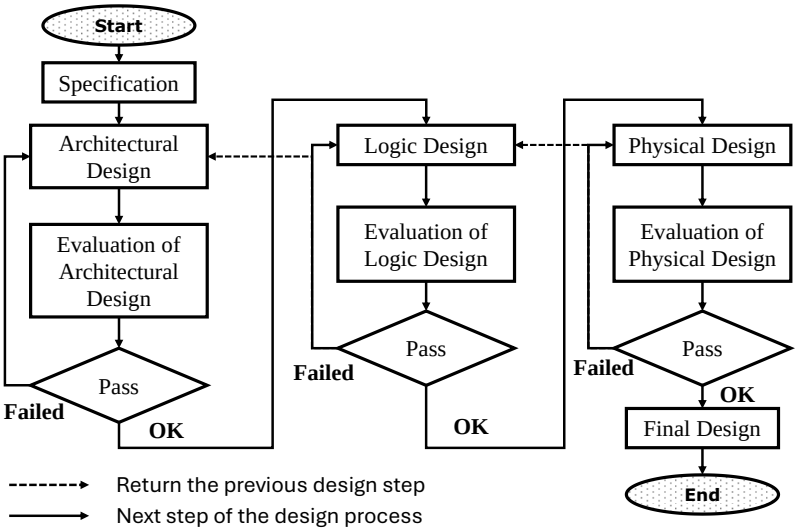


Figure 2.2: Regular Top-down Design Methodology for Hardware Design.

2.2 Traditional Design Methodology for Hardware Implementation

2.2.1 Top-down Design Flow

In digital circuit design, particularly for cryptographic applications such as ECC primitives, the top-down design approach has emerged as the most popular and widely adopted methodology, as demonstrated in Figure 2.2.

This section presents both the pros and cons of utilizing the top-down design process in practice. The main disadvantage of the Top-down design approach is insufficient granularity in sub-block architecture at the beginning design stages, which often delays verification of compliance with critical constraints until the later stages. Additionally, incorporating the countermeasures at the end of the process inflates the implementation costs. Alternatively, redesigning to meet security demands extends the time-to-market costs. Thus, it necessitates careful trade-offs to balance security, cost, and time-to-product issues.

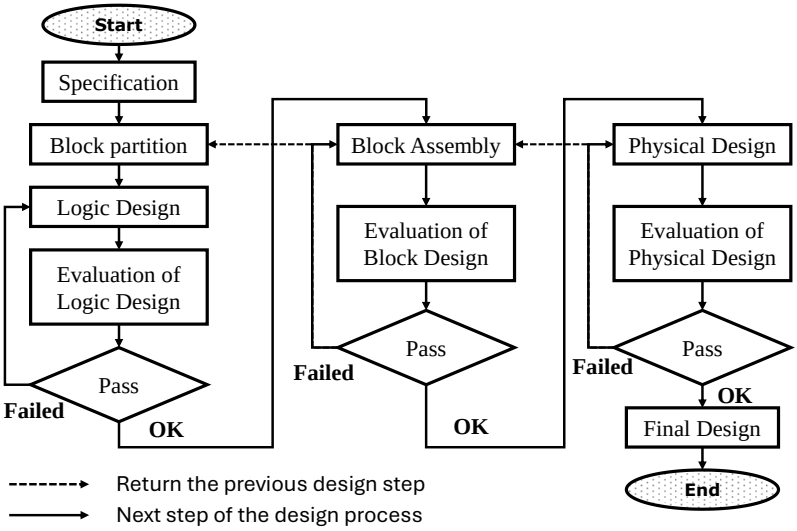


Figure 2.4: Regular Bottom-up Design Methodology for Hardware Design.

2.2.2 Bottom-up Design Flow

An alternative design methodology is the Bottom-up process. Distinguished by the Top-down design flow, this process enables the simplicity of localized evaluation, as depicted in Figure 2.4.

This section also reviews the disadvantages and advantages of the Bottom-up Design Process. Firstly, independently optimized sub-blocks often result in irregular shapes, leading to die-core fragmentation and underutilized silicon area. Second, the reliance on abstract models during assembly introduces inaccuracies; a sub-block local power estimate might neglect global voltage drop effects, compromising system-level predictions. Furthermore, the exhaustive simulations required in the last design stage become impractical for complex ECC systems.

2.2.3 Emerging AI-Driven Design Methodologies

In the realm of Artificial Intelligence, the generative AI model plays a critical role as an assistant to the designer in optimizing the implemented hardware systems. Several AI-driven Design Methodologies are under consideration in this section. Their benefits and drawbacks are also presented.

2.3 Design Methodology for Hardware Security Design

In a particular application of implemented design, the complementary stages are supplemented into the original design flow, enabling the designer to quickly evaluate and modify the system to fit the design constraints. This section provides an overview of the complementary security evaluation for the ECC-based authentication system, which is constructed using the Top-down design methodology.

2.3.1 Complementary Security Evaluation for Design Methodologies

Adapting to the security hardware design, the designer complements the security evaluation of all necessary vulnerabilities at the end of the original Top-down design approach. In the first approach, after fabricating the hardware design, the designers take into account experiments to measure the security level of the implemented system. One of the key advantages of this method lies in its precision, but the main drawback of this method is the complicated processes for meticulous

signal calibration and synchronization. Achieving reliable results requires substantial computational resources and domain expertise. In addition, if a security evaluation fails, designers must go back to the beginning, where the alternative RTL design with countermeasures will be proposed. This loopback of reconstructing the alternative secured system causes a critical problem. Designing alternative solutions and prototypes takes more time and costs more.

The second approach to evaluate the security of the design methodologies is post-synthesis security evaluation. Although enabling the reduction in the dependency on costly and time-consuming post-silicon evaluations, the post-synthesis security evaluation approach also faces several issues. Firstly, the limitations of simulation must be acknowledged: factors like process variations, interconnect parasitics, and environmental noise are abstracted away, leading to discrepancies between simulated and physical traces. Besides, power traces harvested at the gate level also cause a storage problem as the file size contains power traces. This leads the evaluation engine to arrange a large storage and processing capacity for analysis.

2.3.2 Security Evaluation for Secured RFID Tags

This section emphasizes distinct approaches for evaluating security at both the protocol and hardware levels. For the protocol level, the evaluation focuses on assessing the security of RFID (Radio Frequency Identification) tags that are resistant to unauthorized access. These evaluations analyze the ability of security protocols to counter wireless threats and maintain optimal system performance. At the hardware security level, the susceptibility of a design to side-channel attacks (SCAs), which exploit unintended physical emissions—such as power fluctuations or electromagnetic radiation—to extract sensitive data like encryption keys, is quantified by using Test Vector Leakage Assessment or Power Analyses tools.

Conclusion

This thesis chapter reviews the existing design methodologies in general hardware implementation before the practical design process in the secured RFID tags. The existing design flows are analyzed to highlight both advantages and disadvantages. In general, almost all of them face the high time-to-product problem, which significantly impacts the

manufacturing cost of the products. Besides, relegating the countermeasures to the late design stages risks suboptimal trade-offs, as late-stage security adjustments may necessitate costly redesigns or compromises in system efficiency. Recent advancements in AI-based Automatic Design Space Exploration (DSE) offer promising solutions to this challenge. However, they often treat security as a static constraint rather than a dynamic, co-equal parameter to be actively optimized during the design process. By analyzing these existing design methodologies, this thesis chapter figures out the gap, underscoring the need for a paradigm shift: embedding security-aware co-optimization into AI-driven DSE frameworks. This thesis addresses this limitation by proposing a novel methodology that integrates real-time security evaluation metrics and implementation cost estimation directly into the DSE loop, which is presented in more detail in Chapter 4.

Chapter 3

Hardware Implementation of Elliptic Curve Cryptography

A balanced design, which is a compromise between the implementation cost and the security level against wireless attack and hardware attacks, is a challenge for the designers to implement by utilizing the design methodologies presented in Chapter 1. In this chapter, we propose a low-cost, low-power hardware implementation of Elliptic Curve Cryptography using the Top-down design methodology.

3.1 Related works

3.1.1 Optimizing the implementation cost on ECC

This thesis section reviews the state-of-the-art methods of optimizing the implementation cost of the ECC. The reviewed approaches include the selection of lightweight curves, utilizing the Binary Field $GF(2^m)$, Projective Coordinates, and choosing the Gaussian Normal or Polynomial basis field operators. These methodologies are presented to highlight both benefits and drawbacks to highlight the gap in the research.

3.1.2 SCA Security Robustness Improving on ECC

In ECC, point multiplication involves the repeated execution of either point addition or point doubling, depending on the corresponding bit value of the cryptography key. Therefore, utilizing ECC on hardware implementation risks the vulnerabilities of Side-Channel Attacks. To mitigate such vulnerabilities, several countermeasures are proposed in the literature, ranging from selecting a completeness curve to hiding and masking the point multiplication algorithm by dumping the clonable operators. These approaches are also under consideration in this chapter to emphasize the disadvantages of significantly increasing the implementation cost of the system. Consequently, the literature review shows the gap in research on the ECC hardware implementation for passive RFID tags that requires a balance between the hardware implementation cost and the security level.

3.2 The proposed algorithm of Binary Edwards Curves

Addressing the mentioned gap in the literature, this thesis section demonstrates the proposed algorithm of the Binary Edward Curves (BEC).

3.2.1 The Projective ω-coordinate in BEC

Addressing the optimization of BEC's implementation cost, this section presents a solution for a Differential Addition Chain. This approach is analyzed to emphasize the issues of retrieving the x-term, which consumes significant implementation costs.

3.2.2 The Proposed Point Operators using the Projective $\omega-$coordinates in BEC

Due to the high implementation cost of retrieving affine coordinates, the first proposal in this chapter is moving this operator to the severe side to minimize the implementation costs of the passive RFID tags. Furthermore, to reduce the implementation cost of the point operators, the second proposal alternates the conventional operators by Equation (3.1).

$$\begin{aligned} \frac{W_3}{Z_3} &= \frac{C + \frac{1}{\omega_0} \cdot C}{(Z_1 Z_2)^2 + \frac{1}{\omega_0} \cdot C} \\ \frac{W_4}{Z_4} &= \frac{A}{d \cdot (Z_1 \cdot Z_1)^2 + A} \end{aligned} \tag{3.1}$$

3.3 The proposed Hardware Architecture of Binary Edwards Curves

3.3.1 The Proposed System Architecture of BECs

This section presents the third proposal in this chapter by a systematic architecture of low-cost, low-power BEC, as demonstrated in Figure 3.2. The detailed illustration of the third proposal is described in this section to highlight the proposed Arithmetic Computation Block.

3.3.2 The Proposed Arithmetic Computation Block

An integrated block of arithmetic computation (ACB) is proposed to process the field multiplier and field square immediately, as depicted in Figure 3.5, to minimize the number of registers. A detailed illustration of the proposed ACB block is presented in this section.

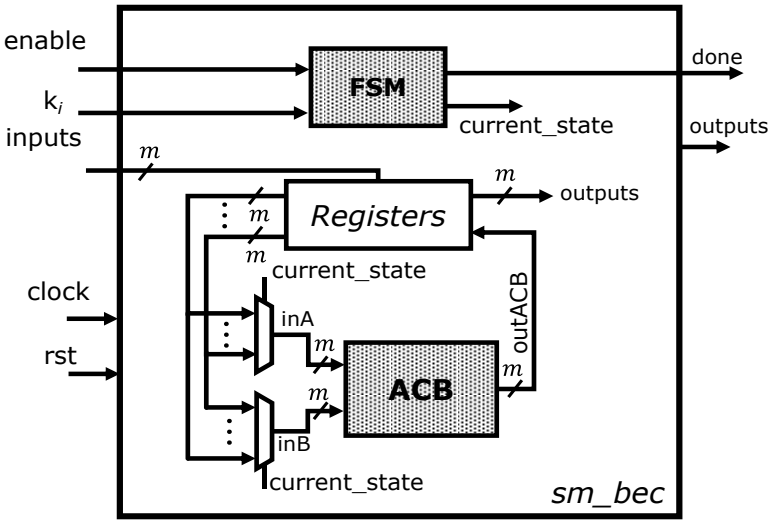


Figure 3.2: Proposed low-cost, low-power architecture of Binary Edwards Curve using bit-serial processing.

3.4 Hardware Implementation Results

3.4.1 Experimental Setup

In this section, the implementation of the proposed design of BEC architecture will be presented. The implementation cost and the security properties of the proposed BEC design will also be provided and discussed to demonstrate the experimental conditions.

3.4.2 Hardware Implementation Results

The experiments are carried out by Synopsys Electronic Design Automation (EDA) tools such as Design Compiler and PrimeTime with the CMOS 65nm from TSMC. The operational frequency ranging from $10MHz$ to $0.4MHz$ shows the comparative power consumption at $4.66\mu W@0.4MHz$. The highest performance of the proposal is also considerable for passive RFID tags with a latency of $19.05ms@10MHz$.

3.4.3 Security Evaluation

Regarding the security evaluation, the hardware implementation is evaluated using the TVLA test. Nevertheless, the maximum leakage is

quantified at 3.36, which is smaller than the standard threshold of 4.5. Thus, the proposed design is secured against the SCA.

Conclusion

This section of the thesis proposes a low-cost, low-power architecture with a modified algorithm of point multiplication of BEC. The main contributions of this chapter involve:

- **Removing the retrieving step into the affine coordinate**.
- **Proposed field operators**.
- **Proposed BEC architecture along with proposed Arithmetic Computation Block**.

According to the synthesis results within the CMOS 65nm technology library from TSMC, the proposed BEC provides a low-cost, low-power, and secured design against SCA threats. However, by utilizing the conventional top-down design methodology, the time-to-production is as large as the repetition in selecting the design. Additionally, the late supplementing of the security countermeasure prevents the designers from considering both security and the implementation cost early in the design process.

Chapter 4

Proposed Early Evaluation Design Methodology

4.1 Introduction

The paragraph discusses the challenge of time-to-production in VLSI design, particularly for security hardware. It critiques traditional design methods for treating security as a secondary concern, leading to difficulties in balancing security requirements with implementation costs. The chapter proposes a new design methodology to address this issue.

4.2 Proposed Early Evaluation Design Methodology

4.2.1 Meet-in-the-Middle Design Process

The proposed Meet-in-the-Middle (EEMitM) necessitates initial design specifications, which are utilized as the foundational criteria for the systematic evaluation. These quantification metrics enable an early analysis and optimization mechanism of the proposed design methodology, as described in Figure 4.1. This section provides an insight into the proposal.

4.2.2 Bottom-Up Verification and Validation Process

This thesis section describes the proposed Bottom-up Verification and Validation Process (B2VP)to validate the hardware implementations of field operators and foundational security primitives.

4.3 The Proposed Pseudo Power Traces Generation Methodology

4.3.1 Power Consumption Analysis

A novel security evaluation methodology, utilizing the Man-in-the-Middle (EEMitM) design framework, is introduced in this thesis section to evaluate the leakage of the system. In this section, a theoretical analysis of the systematic power consumption is presented to highlight the proposed estimation mechanism.

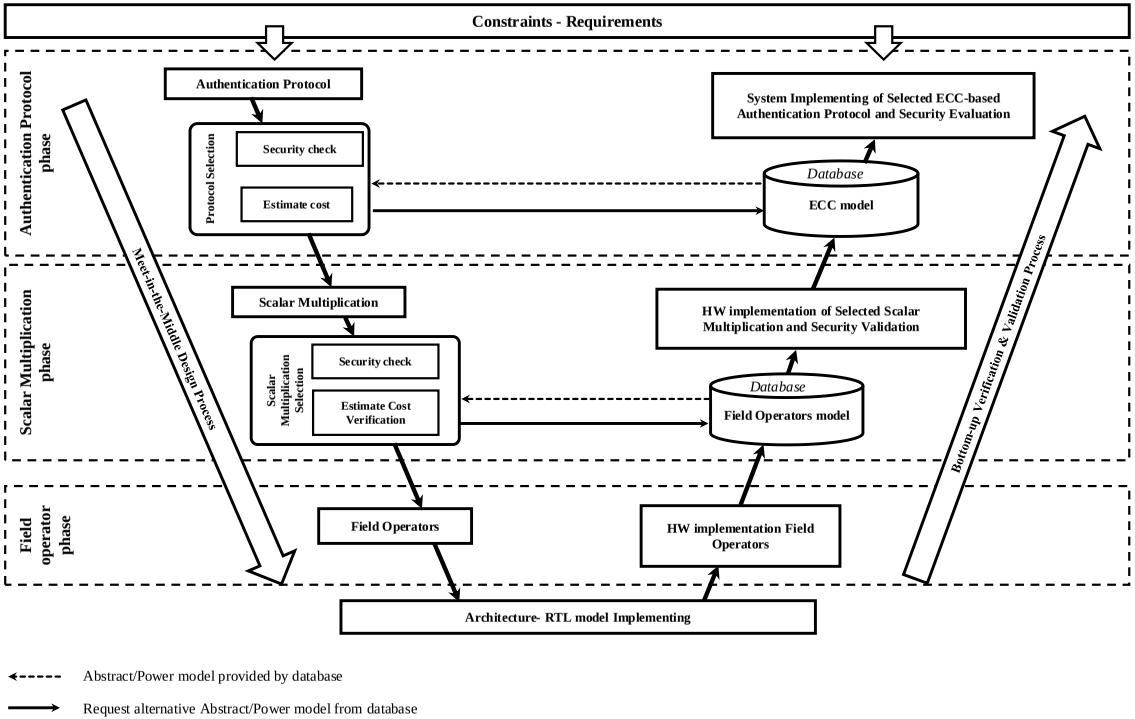


Figure 4.1: Proposed Early Evaluation Design Methodology.

4.3.2 Systematic Power Model

This section presents the proposed approach that facilitates the estimation of pseudo-power traces for cryptographic primitives without necessitating extensive physical measurements. There are two proposed approaches are described in this thesis section:

- **Forming based on the sub-traces of the components**.
- **Resulting from the function of switching activity**.

4.4 Evaluation Results

4.4.1 Experimental Setups

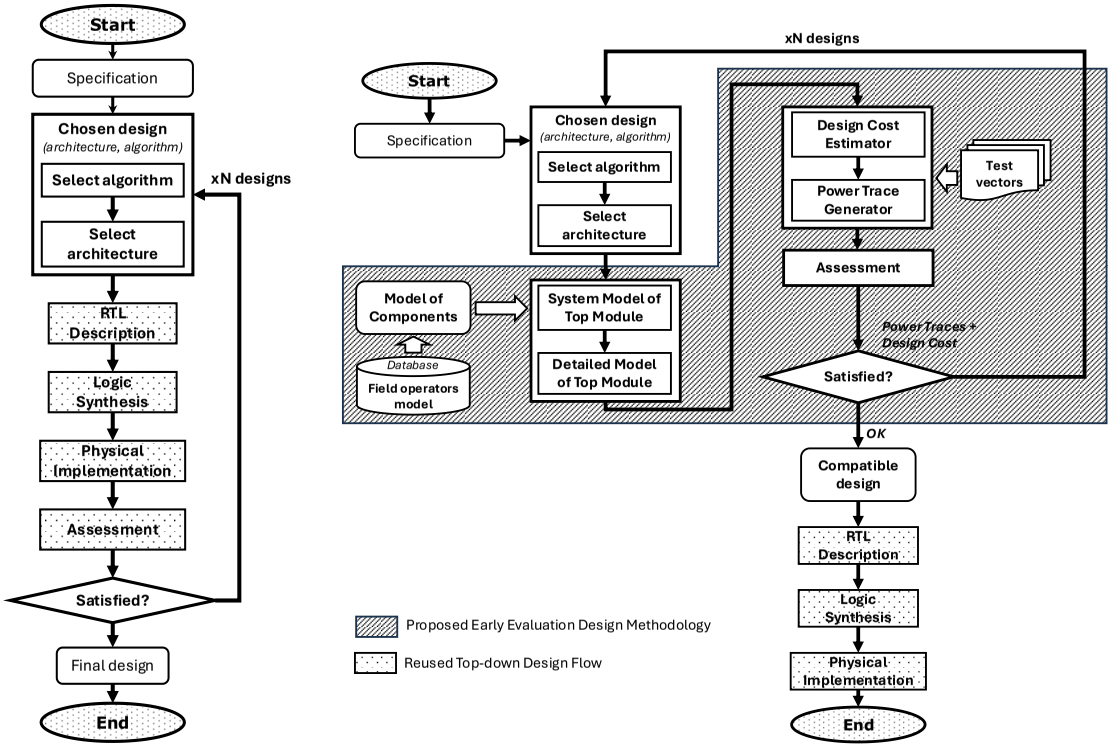
To evaluate the accuracy and efficiency of the proposed EEMitM design methodology, several experiments are designed to quantify the implementation costs performance metrics, security levels, and time-to-product efficiency of the proposed design methodology and the conventional design approach. The experimental setup involved applying both the proposed and conventional methodologies to design ECC-based authentication protocols under identical constraints, as demonstrated in Figure 4.14.

4.4.2 Results of Experiments for Protocol Stages Design and Evaluation Stages

The paragraph discusses the evaluation of low-cost, energy-efficient ECC hardware for authentication protocols, revealing that none meet passive RFID tag latency requirements. It also highlights ongoing efforts to optimize security primitives within defined design constraints

4.4.3 Results of Experiments for Security Primitive Design and Evaluation Stages

After executing the protocol stage, the security primitive design stage is performed to continue optimizing with the determined resource constraints. The evaluation results show that the Dual Processing Elements (PEs) architecture yields a better $APT2$ benchmark score, demonstrating a more optimal balance between cost and performance despite the increased resource utilization.



(a) Conventional Top-down Hardware Design Flows.

(b) Proposed EEMitM for Hardware Implementation.

Figure 4.14: Description level of design in Top-down Design methodology.

Regarding the accuracy of the estimation mechanism, the proposed approach shows a perfect alignment between estimation and EDA results, with identical ratios of 1.75 and minimal error margins of 1.2% (Single) and 1.1% (Dual). Overall, the estimation results show a strong correlation with EDA outputs, particularly for area and latency metrics, validating the estimation methodology's effectiveness.

Conclusion

By using the proposed innovative design methodology, the estimation and evaluation are executed over the software with the determined database in the duration of $T_{SW} << T_{HW}$. At the end of the assessment, the optimal design is implemented on hardware within T_{HW}. In total, the time-to-product of using the proposed EEMitM design methodology is $N \cdot T_{SW} + T_{HW}$.

Related to the precision of the estimation, the proposal provides an impressive accuracy of 1.2% of error in latency. In the worst estimation of the power consumption, the accuracy stays at an acceptable error of 22.6%.

Conclusion and Future Works

With the outstanding advantages of low cost and low power, ECC-based passive RFID tags have become an essential part of our lives, ranging from civil to military applications, significantly impacting human daily life. However, these recent attempts contain limitations as follows:

- The conventional attempts often treat security as an afterthought or a complementary feature at the later design phase rather than concerning it at the beginning. Consequently, the ability to produce insecure and costly ECC-based solutions.

- Due to the massive design space, the conventional design methodology, which implements trial-and-error to find the optimal design, consumes a huge time-to-product cost.

Addressing these mentioned drawbacks, the ultimate goal of this research was to propose a comprehensive set of design phases that enable the designer to quickly and early estimate, evaluate, and choose the best systematic configurations for hardware implementation. Consequently, the designers save the time-to-product cost. The main research works can be summarized briefly as follows:

1. A 21.68 $kGates$ of a low-cost, low-power hardware architecture of BEC has been proposed and synthesized by using the CMOS TSMC 65nm technology, according to the conventional Top-down design methodology. The proposed hardware implementation consumes $126\mu W@10MHz$ of power, estimated by the Synopsys PrimeTime tool. The hardware implementation results of the proposal show that our proposed system is efficient in terms of implementation cost and energy consumption when compared with other works. Besides, the TVLA evaluation proves that the proposal is secure against side-channel vulnerabilities. These results are published in [C1].

2. To solve the problem of time-to-product, we proposed the Early Evaluation MitM design methodology. By using the database

of the reference security primitives, the designers can possibly model the chosen system without prototyping. The proposed framework enables quick modeling over the software environment, which significantly reduces the time to produce. The experiments show that by applying the proposal, the time-to-product reduces by 480 times compared to the conventional design flow. Regarding the accuracy of the estimation of implementation costs, the experiments show a precise estimation of 1.2% of error in latency. In the worst estimation of the power consumption, the accuracy stays at an acceptable error of 22.6%. These discussions of the proposal are published in [C2, C3, P1] and partly presented in [J1].

While this study has made strides in addressing key challenges within the exploration of the design space for ECC (Elliptic Curve Cryptography)-based authentication protocols tailored to passive RFID (Radio-Frequency Identification) tags, several avenues for future research remain open. However, to advance the field further, the following directions are proposed as critical next steps.

1. **Evaluate the security properties**

2. **Develop Commercial EDA Tools with the proposed EEMitM design methodology**

3. **Extending Application-Specific Database**

List of Publications

List of publications relevant to the thesis

C1 **Manh-Hiep Dao**, Vincent Beroulle, Yann Kieffer, Xuan-Tu Tran, and Duy-Hieu Bui. "Low-cost Low-Power Implementation of Binary Edwards Curve for Secure Passive RFID Tags." In 2023 IEEE 16th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), pp. 494-500. IEEE, 2023.

C2 **Manh-Hiep Dao**, Vincent Beroulle, Yann Kieffer, and Xuan-Tu Tran. "How to Develop ECC-Based Low-Cost RFID Tags Robust Against Side-Channel Attacks." In International Conference on Industrial Networks and Intelligent Systems, pp. 433-447. Cham: Springer International Publishing, 2021.

C3 **Manh-Hiep Dao**, Vincent Beroulle, Yann Kieffer, and Xuan-Tu Tran (2023). Secure-by-Design methodology using Meet-in-the-Middle design flow for hardware implementations of ECC-based passive RFID tags. In ICWMC 2023, The Nineteenth International Conference on Wireless and Mobile Communications. IARIA (pp. 14-19).

J1 Souhir Gabsi, Vincent Beroulle, Yann Kieffer, **Manh-Hiep Dao**, Yassin Kortli, and Belgacem Hamdi. "Survey: Vulnerability analysis of low-cost ECC-based RFID protocols against wireless and side-channel attacks." Sensors 21, no. 17 (2021): 5824. (**SCIE, Q2**).

P1 **Đào Mạnh Hiệp**(2023), "Quy trình thiết kế phần cứng bảo mật cân bằng giữa chi phí thực thi và mức độ bảo mật" (VN Patent No. 1-2023-06893) (*Accepted*)

List of publications published during the thesis

J2 **Manh-Hiep Dao**, Koichiro Ishibashi, The-Anh Nguyen, Duy-Hieu Bui, Hiroshi Hirayma, Tuan-Anh Tran, and Xuan-Tu Tran. "Low-cost, High Accuracy, and Long Communication Range Energy-

Harvesting Beat Sensor with LoRa and Ω-Antenna for Water-Level Monitoring." IEEE Sensors Journal (2025). (**SCIE, Q1**).