STUDIES PUBLICAÇÕES
Studies in Engineering and Exact Sciences
ISSN: 2764-0981

Performance evaluation and analysis of public-key schemes in embedded IoT devices

Avaliação de desempenho e análise de esquemas de chave pública em dispositivos IoT embarcados

Evaluación y análisis de rendimiento de esquemas de criptografía de clave pública en dispositivos IoT incorporados

DOI: 10.54021/seesv5n2-214

Originals received: 08/16/2024
Acceptance for publication: 09/06/2024

Fares Mezrag
Doctor in Computer Science
Institution: Department of Computer Science, University of M'Sila
Address: M'Sila 28000, Algeria
E-mail : fares.mezrag@univ-msila.dz

Abderrahim Zemmit
Doctor in Electrical Engineering
Institution: Department of Electrical Engineering, University of M'Sila
Address: M'Sila 28000, Algeria
E-mail : abderrahim.zemmit@univ-msila.dz

ABSTRACT

The Internet of Things (IoT) is considered one of the emerging technologies that have attracted widespread attention from industry and academia as a result of their ability to use them in many applications, including military, healthcare, and industrial control. The inherent vulnerabilities in communications of IoT networks, which consist of resource-constrained devices, pose significant security challenges. To protect sensitive data exchanged within these networks, it is necessary to design and implement lightweight and efficient cryptographic schemes that consider resource-constrained IoT devices. This paper evaluates the performance of five well-known public-key schemes on three real-world IoT devices including IOTLAB-M3, Arduino-Zero, and Decawave DWM1001. The examined public-key schemes are categorized into two classes: integer factorization-based (RSA and Rabin schemes) and elliptic curve-based (ECIES, ECDH, and ECDSA schemes). By conducting comprehensive experiments, we compare these schemes in terms of computational time and energy consumption, providing valuable insights for selecting optimal public-key schemes in resource-constrained IoT environments.

Keywords: Internet of Things. Data Transmission. Public-Key Cryptography. Elliptic Curve. Integer Factorization. Security.

RESUMO

A Internet das Coisas (IoT) é considerada uma das tecnologias emergentes que têm atraído ampla atenção da indústria e da academia devido à sua capacidade de uso em diversas aplicações, como militar, saúde e controle industrial. As vulnerabilidades inerentes às comunicações das redes IoT, compostas por dispositivos com recursos limitados, representam desafios de segurança significativos. Para proteger dados sensíveis trocados dentro dessas redes, é necessário projetar e implementar esquemas criptográficos leves e eficientes que considerem os dispositivos IoT com recursos limitados. Este artigo avalia o desempenho de cinco esquemas de chave pública bem conhecidos em três dispositivos IoT do mundo real, incluindo IOTLAB-M3, Arduino-Zero e Decawave DWM1001. Os esquemas de chave pública examinados são categorizados em duas classes : baseados em fatoração inteira (esquemas RSA e Rabin) e baseados em curva elíptica (esquemas ECIES, ECDH e ECDSA). Por meio de experimentos abrangentes, comparamos esses esquemas em termos de tempo de computação e consumo de energia, fornecendo insights valiosos para a seleção de esquemas de chave pública ótimos em ambientes IoT com recursos limitados.

Palavras-chave: Internet das Coisas. Transmissão de Dados. Criptografia de Chave Pública. Curva Elíptica. Fatoração Inteira. Segurança.

RESUMEN

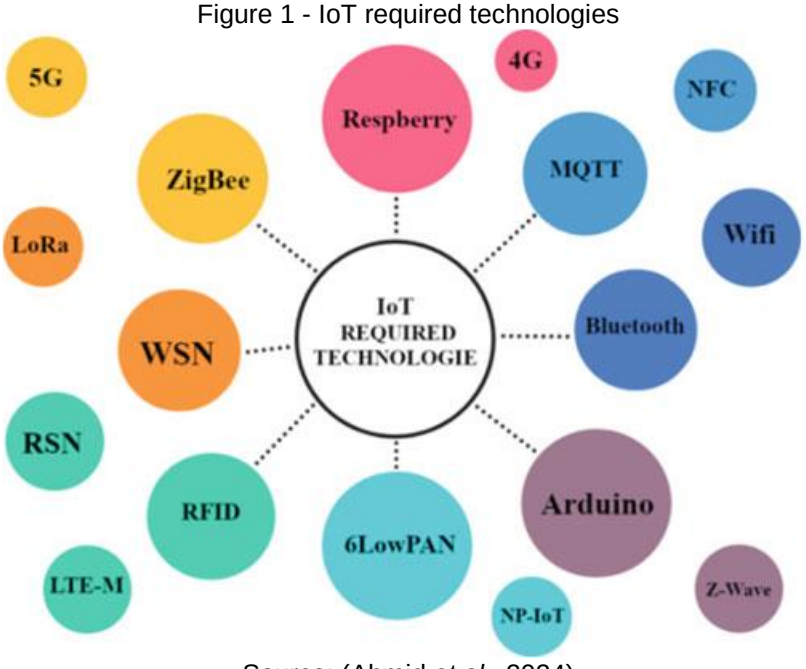
La Internet de las Cosas (IoT) es considerada una de las tecnologías emergentes que ha atraído amplia atención de la industria y la academia debido a su capacidad de uso en diversas aplicaciones, como militar, salud y control industrial. Las vulnerabilidades inherentes a las comunicaciones de las redes IoT, compuestas por dispositivos con recursos limitados, representan desafíos de seguridad significativos. Para proteger datos sensibles intercambiados dentro de estas redes, es necesario diseñar e implementar esquemas criptográficos ligeros y eficientes que consideren los dispositivos IoT con recursos limitados. Este artículo evalúa el rendimiento de cinco esquemas de clave pública bien conocidos en tres dispositivos IoT del mundo real, incluyendo IOTLAB-M3, Arduino-Zero y Decawave DWM1001. Los esquemas de clave pública examinados se clasifican en dos categorías: basados en factorización entera (esquemas RSA y Rabin) y basados en curva elíptica (esquemas ECIES, ECDH y ECDSA). Mediante experimentos exhaustivos, comparamos estos esquemas en términos de tiempo de computación y consumo de energía, proporcionando valiosos conocimientos para la selección de esquemas de clave pública óptimos en entornos IoT con recursos limitados.

Palabras clave: Internet de las Cosas. Transmisión de Datos. Criptografía de Clave Pública. Curva Elíptica. Factorización Entera. Seguridad.

1 INTRODUCTION

Kevin Ashton introduced the Internet of Things (IoT) in 1999. This concept envisions a world where any object can be connected to the internet and communicate with other devices, regardless of location or size (Gubbi *et al*., 2013). IoT devices are equipped with sensors to collect data and actuators to perform actions autonomously. In recent years, the IoT has gained significant attention due to its potential to benefit humans in countless ways. Applications span a wide range of areas, including home automation, environmental monitoring, and healthcare (Vermesan *et al*., 2013). The IoT is realized through the integration of various technologies and protocols, such as Wireless Sensor Networks (WSN), Radio Frequency Identification (RFID), cloud computing, and Constrained Application Protocol. Consequently, IoT inherits the security vulnerabilities inherent in these constituent technologies (Ahmid *et al*., 2024). Some available technologies are illustrated in Figure 1.

Figure 1 - IoT required technologies



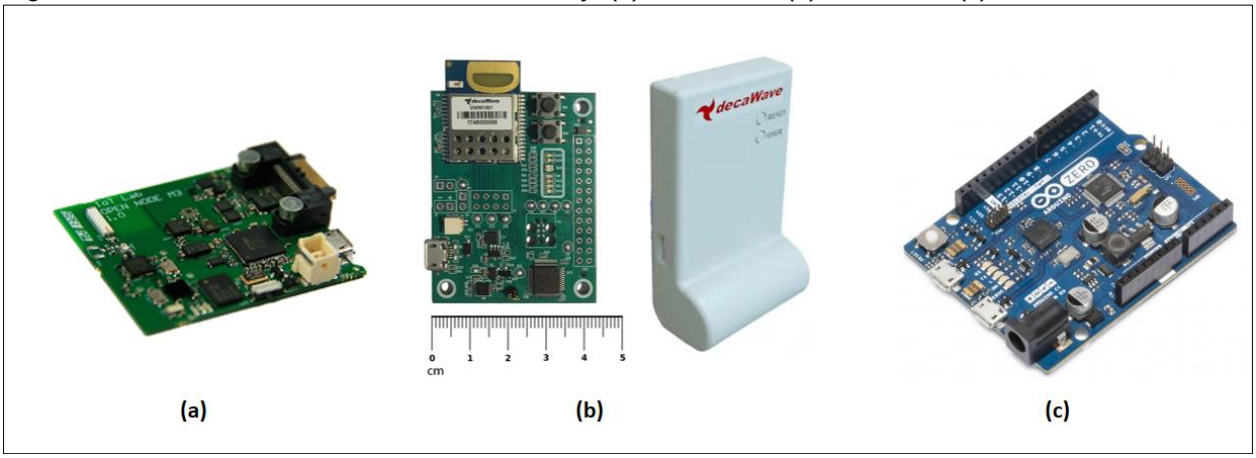
Source: (Ahmid *et al*., 2024)

Cyber-attacks and unauthorized access are prevented by a network's security policies, mechanisms, and services. IoT networks face several security challenges, particularly when it comes to applications requiring high levels of security, such as military, emergency response, and healthcare applications. With

regard to the WSN scenario, sensor devices are frequently deployed in hostile or even unsecure environments, making them more vulnerable to cyber-attacks that could result in the violation of sensitive data and adversely affect network performance. Additionally, wireless communication within IoT networks is by nature insecure, so an adversary with a wireless device can easily listen in on legitimate IoT communications. Thus, it is necessary to ensure minimal security requirements such as authentication, data confidentiality, and data integrity. Additionally, lightweight, efficient, and secure schemes must be designed that take into account the limited resources of IoT devices.

Security requirements, such as confidentiality, integrity of data, authentication, and nonrepudiation, are guaranteed by cryptography. There are generally two types of cryptographic techniques, which are Symmetric Key Cryptography (SKC) and Public Key Cryptography (PKC). Despite the fact that a solution based on SKC has a low computational overhead and energy consumption, distributing keys is a more complex and difficult process. A PKC-based solution provides greater flexibility by making key distribution easier and non-repudiation possible, however, they are computationally expensive for resource-constrained sensor nodes (Zhao *et al*., 2011). According to recent papers (Boudia *et al*., 2015); (Mezrag *et al*, 2017, 2019, 2022); (Murthy *et al*., 2012), the application of PKC on resource-constrained device is feasible. This paper assesses the performance of well-known public-key cryptographic schemes on constrained wireless devices. Specifically, we evaluate computational time and energy consumption on three popular IEEE 802.15.4-compliant IoT hardware platforms: IOTLAB-M3 (FIT-IOT-LAB, 2024), Arduino-zero (Arduino, 2024), and DWM1001 (DecaWave, 2024). Figure 2 presents the three IoT hardware devices used in this study. A detailed comparison of their specifications can be found in Table 1.

Figure 2 - IoT hardware devices used in this study. (a) IoTLab-M3 (b) Decawave (c) Arduino-zero



Source: Authors

We examine five public-key schemes: RSA (Rivest *et al.*, 1978) and Rabin (Rabin, 1979) (integer factorization-based) and ECDH (Hankerson *et al*., 2021), ECDSA (Hankerson *et al*., 2021), and ECIES (Hankerson *et al.*, 2021) (elliptic curve-based). By comparing computational performance and energy consumption, we provide insights for selecting optimal public-key schemes in resource-constrained IoT environments.

Table 1 - List of IoT boards Used for Experimentation.

IoT device Boards	IOTLAB-M3	Arduino zero	Decawave DWM1001
MCU	STM32, 32 bits ARM Cortex M3	ATSAMD21G18, 32-Bit ARM Cortex M0+	nRF52832, 32 bits ARM Cortex-M4
SRAM	64 KB	32KB	64KB
Flash	256 KB	256KB	512KB
Battery	3,3V Li-Po battery, 650 mAh	3.3V Li-Po single cell, 700 mAh	3.6V Li-Ion 650 mAh
Current consumption	6.4 mA	3.7 mA	3.3 mA
Radio	2.4-GHz IEEE 802.15.4 & Zigbee compliant.	2.4-GHz IEEE 802.15.4 (XBee module)	2.4-GHz IEEE 802.15.4 & Zigbee compliant.
Operating-Systems	FreeRTOS, Contiki, RIOT	RIOT, Zephyr	RIOT

Source: Authors.

1.1 CONTRIBUTION

The main contribution of our study is:

- *Guiding Algorithm Selection for Secure IoT Communications*: The study offers practical advice for developers and security engineers working on IoT

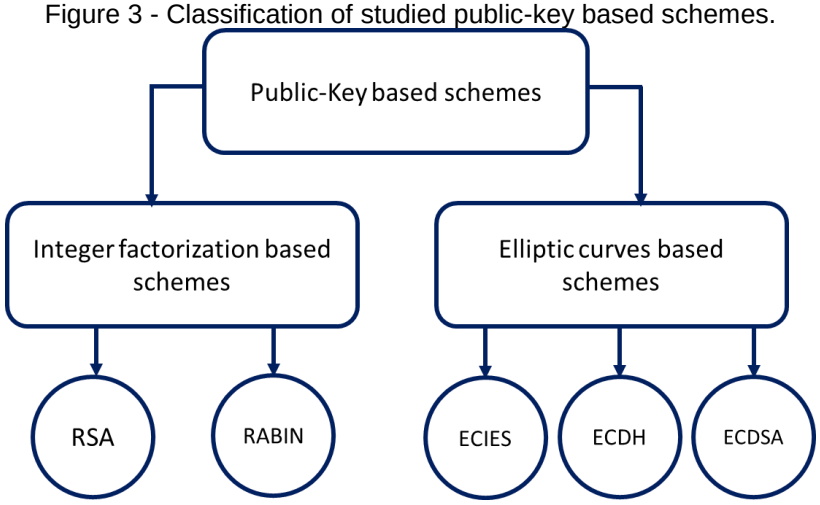
systems. By comparing the performance of RSA, Rabin, ECIES, ECDSA, and ECDH, the research helps in identifying the energy-efficient and computationally lightweight schemes. Thus, the research helps in selecting the most appropriate algorithms for specific IoT applications and resource limitations.

The remainder of this paper is organized as follows: Section 2 provides a classification of the studied public-key based schemes. Experimental results and their analysis are presented in Section 3. Finally, Section 4 concludes the paper.

2 CLASSIFICATION OF PUBLIC-KEY BASED SCHEMES

We can classify the studied public based key schemes into two categories: integer factorization based and elliptic curves based, as shown in Figure 3.

Figure 3 - Classification of studied public-key based schemes.



Source: Authors

2.1 SCHEMES BASED ON INTEGER FACTORIZATION

The difficulty of factoring large integers into their prime factors has been a cornerstone in the development of modern cryptography. Several cryptographic schemes rely on this computational challenge for their security. Some of these schemes are mentioned in this paper: RSA and Rabin schemes (Rabin, 1979); (Rivest *et al*.,1978).

2.1.1 RSA scheme

RSA is an asymmetric cryptographic algorithm introduced by Rivest, Shamir, and Adleman Rivest *et al*. (1978). RSA relies on the difficulty of factoring large integers for its security. To achieve this, it employs a massive integer, N, from which a public key (e) and a private key (d) are derived. Encryption is performed using the public key, while decryption requires the corresponding private key. The security of RSA is directly correlated to the size of the integer N: larger integers equate to stronger security. However, this enhanced security comes at the cost of increased computational overhead.

2.1.2 Rabin scheme

Rabin scheme is a public-key cryptosystem invented by Michael Rabin (1979). The Rabin cryptosystem is a public-key encryption system based on the difficulty of integer factorization. Its security is proven equivalent to the problem of factoring large integers, a challenge that underpins many modern cryptographic systems. Rabin scheme consists of three phases: Key generation, Encryption and Decryption.

Key generation:

1. Choose two large distinct prime numbers p and q.
2. Calculate the modulus $n = p.q$
3. Publish n as public key and save p and q as private key

Encryption:

Given a plaintext message m, the cipher text c is calculated as: $c = m^2 \ mod \ n$.

Decryption:

Decryption in the Rabin scheme is more complex than encryption due to the nature of the square root operation modulo n. There are four possible values for the square root of a number modulo n. Therefore, additional techniques are required to determine the correct plaintext.

2.2 SCHEMES BASED ON ELLIPTIC CURVES

Elliptic Curve Cryptography (ECC) is a public-key cryptosystem built upon the algebraic structure of elliptic curves defined over finite fields. Due to its efficiency in resource-constrained environments, ECC offers equivalent security to traditional systems like RSA while using a significantly shorter key size. Fundamentally, ECC operates over a finite field Fq, where q is a large prime number. An elliptic curve E defined over Fq is represented by the simplified Weierstrass equation (Hankerson *et al.*, 2021): $y^2 = x^3 + ax + b$, where $a, b \in$ Fq and $4a^3 + 27b^2 \neq 0$.

In the following sections, we describe well-known ECC schemes, including a key agreement (ECDH), public-key encryption (ECIES), and a digital signature (ECDSA). Suppose that *E* is the elliptic curve over a finite field F_q and *G* represents the generator point on the curve.

2.2.1 ECDH scheme

ECDH is a key exchange mechanism based on elliptic curves helping two parties establish a shared secret key (Pairwise Key) through an open and insecure channel. Alice secretly selects an integer k_A (as private key) and computes the point $Q_A = k_A.G$ (as public key) which will be sent to Bob. In turn, Bob secretly chooses k_B and computes $Q_B = k_B.G$ that will be sent to Alice. Both parties compute the shared key: $sk = k_A.Q_B = k_B.Q_A = k_A.k_B.G$.

2.2.2 ECIES scheme

ECIES is a public-key encryption scheme based on ECC. The scheme is designed to be semantically secure in the presence of an adversary capable of launching chosen-plaintext and chosen-cipher text attacks. Please refer to (Brown, 2009) for further details. Next, we demonstrate how to exchange a message using ECIES. To send an encrypted message to Bob using ECIES, Alice needs the following information:

- The cryptography suite to be used, including Key Derivation Function (KDF), a Message Authentication Code (MAC), and a symmetric encryption scheme such as AES.
- The Bob's public key $Q_B = k_B.G$, where $k_B \in Z^*_q$ is the Bob's private key (randomly selected).
- Shared information S1 and S2.

In Table 2, the steps that Alice and Bob must follow to encrypt and decrypt the message m. Note that $x(r.Q_B)$ returns the x-coordinate of an elliptic curve point $r.Q_B$

Table 2 - ECIES scheme: encryption/decryption.

To encrypt a message m by Alice	**To decrypt a ciphertext $R\|\|c\|\|d$ by Bob**
1 - Picks a random number $r \in \mathbb{Z}_q^*$	1 - Computes $S = x(k_B.R)$
2 - Computes $R = r.G$	2- Computes $k_E\|\|k_M = KDF(S\|\|S_1)$
3 - Computes $S = x(r.Q_B)$	3 - Computes $\overline{d} = MAC(k_M, c\|\|S_2)$
4 - Computes $k_E\|\|k_M = KDF(S\|\|S_1)$	4 - Outputs failed if $\overline{d} \neq d$
5 - Computes $c = E(k_E, m)$	5 - If it holds, Bob decrypts the message:
6 - Computes $d = MAC(k_M, c\|\|S_2)$	$m = E^{-1}(k_E, c)$
7 - Send $R\|\|c\|\|d$ to Bob	

Source: Authors

2.2.3 ECDSA scheme

ECDSA is a public-key digital signature scheme based on elliptical curves. Suppose Alice wants to send a signed message to Bob. First, Alice must create a private key $k_A \in Z^*_q$ and a public key $Q_A = k_A.G$. Bob requires Q_A to verify the authenticity of Alice's signature. In Table 3, the steps that Alice and Bob must follow to sign and verify Alice's signature.

Table 3 - ECDSA scheme: signature/verification.

To sign a message m by Alice	To verify Alice's signature by Bob
1 - Computes $z = HASH(m)$	1 - Verify that $r \in \mathbb{Z}_q^*$ and $s \in \mathbb{Z}_q^*$
2 - Picks a random number $k \in \mathbb{Z}_q^*$	2- Computes $z = HASH(m)$
3 - Computes $\overline{X} = x(k.G)$	3 - Computes $u_1 = z.s^{-1} \mod q$
4 - Computes $r = \overline{X} \mod q$	4 - Computes $u_2 = rs^{-1} \mod q$
5 - If $r = 0$, go back to step 2	5 - Computes a point $X = u_1 \times G + u_2 \times Q_A$
6 - Computes $s = k^{-1}(z + r.k_A) \mod q$	6 - Computes $\overline{X} = x(X)$
7 - If $s = 0$, go back to step 2.	7 - The signature is valid if $r \equiv \overline{X} \mod q$
8 - Send (m, r, s)	

Source: Authors

3 EXPERIMENTAL RESULTS AND DISCUSSION

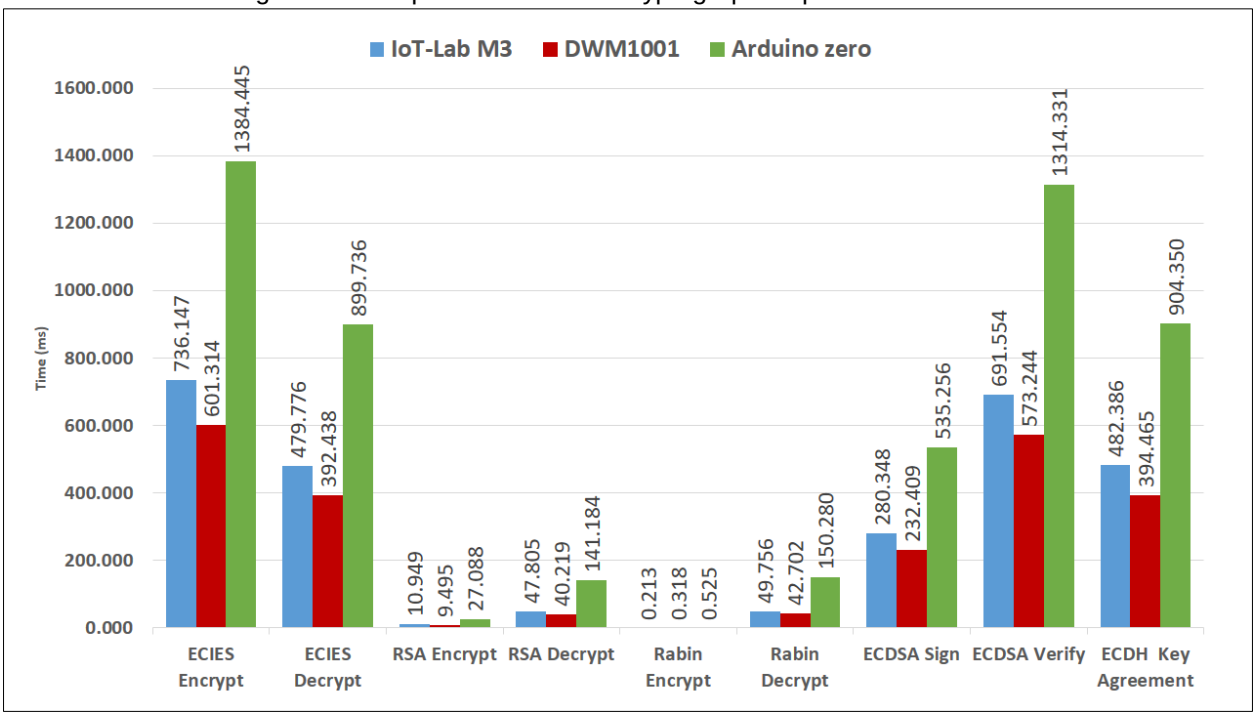
To evaluate the performance of public-key cryptographic schemes, we implemented ECIES, ECDSA, ECDH, RSA, and Rabin within C language and RIOT-OS (Baccelli *et al*., 2018), a lightweight operating system tailored for WSN and IoT environments. Leveraging the RELIC toolkit (Aranha *et al*., 2024), a suitable asymmetric cryptographic library for resource-constrained devices, we employed 3072-bit RSA /Rabin schemes and 256-bit ECC schemes to ensure a 128-bit security level. The performance of studied public-key based schemes was measured on three real-word IoT devices from FIT IoT-LAB testbed (Adjih *et al*., 2015) including, IOTLAB-M3, Arduino-zero, and DWM1001. A detailed comparison of their specifications can be found in Table 1. Two key performance metrics were employed to evaluate the studied PKC schemes: computational cost and energy consumption.

3.1 COMPUTATIONAL COST

Figure 4 illustrates the computational cost, measured in milliseconds, of cryptographic operations performed on IoTLAB-M3, DWM1001, and Arduino Zero boards. Figure 5 presents the time required to generate cryptographic keys, also in milliseconds, for these same IoT boards. As depicted in Figure 4, the Rabin

scheme exhibits the lowest computational time for encryption among the studied schemes, taking 0.213ms, 0.318ms, and 0.525ms on IoTLAB-M3, DWM1001, and Arduino Zero, respectively. Furthermore, we observe that the RSA scheme has a lower decryption time compared to other schemes, with values of 10.949ms, 9.495ms, and 27.088ms on IoTLAB-M3, DWM1001, and Arduino Zero, respectively. Therefore, it can be concluded that the Rabin and RSA schemes offer better computation efficiency compared to ECIES, ECDSA and ECDH schemes.

Figure 4 - Computational cost of cryptographic operations.

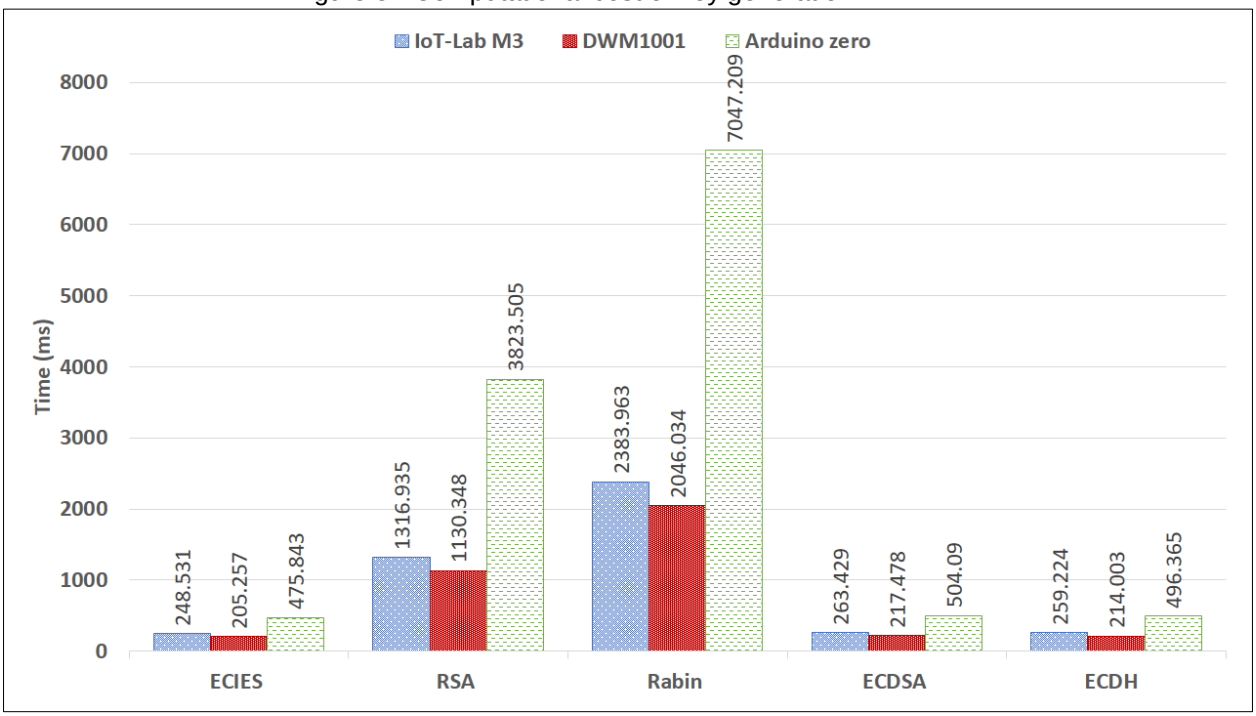


Source: Authors

Conversely, Figure 5 indicates that Rabin and RSA key generation times are substantially longer than those of the three ECC-based schemes. Consequently, RSA and Rabin are less efficient in terms of keys generation time.

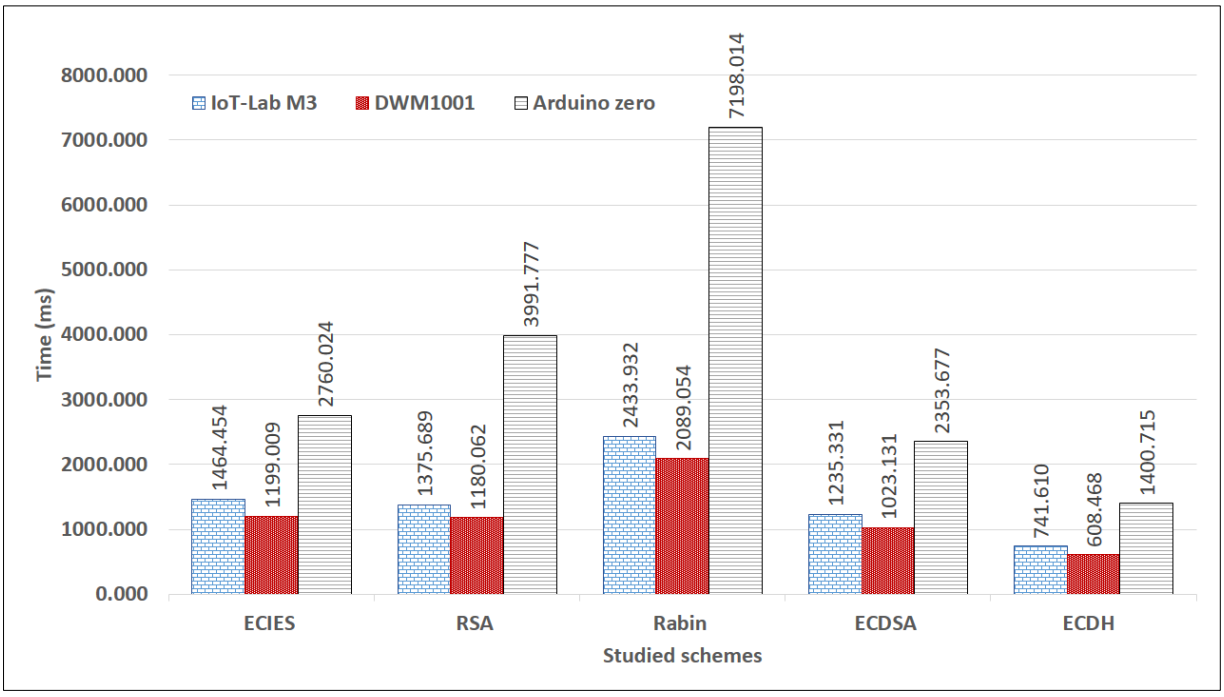
To provide a more comprehensive analysis, the total computation time was determined by summing the key generation time with the cryptographic operations time. The results are illustrated in Figure 6. A comparison of the total computational costs in Figure 6 reveals that Rabin scheme requires high total computational cost than the other schemes. Therefore, Rabin scheme are computationally expensive and not suitable for resource-constrained IoT devices. Regarding the remaining schemes, it can be concluded that they are suitable for limited IoT environments, based on the results shown in Figure 6.

Figure 5 - Computational cost of key generation.



Source: Authors.

Figure 6 - Total Computational cost.



Source: Authors

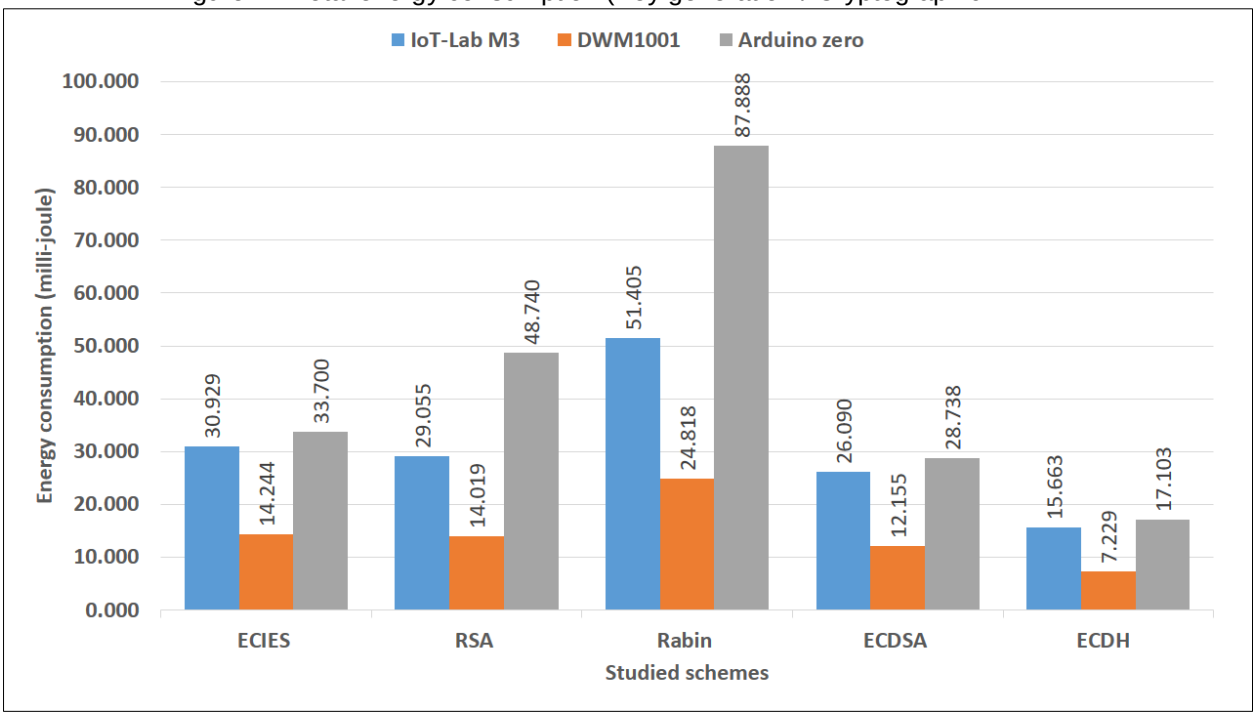
3.2 ENERGY CONSUMPTION

To determine the energy consumed during computation, we applied the

following equation: $W_{comp} = V * C * t$. In this formula, W_{comp} signifies energy in milli-joules (mJ), V represents the supply voltage, C denotes the current consumption during CPU running mode, and t corresponds to the specific runtime in seconds.

Figure 7 presents a comparison of total energy consumption for key generation and cryptographic operations. The data clearly indicates that the Rabin scheme is notably energy inefficient during computations, consuming significantly more energy than other schemes. The primary factor contributing to the Rabin scheme's increased energy consumption is its significantly higher computational cost compared to other schemes. This increased computational cost directly translates to greater energy consumption. Consequently, the Rabin scheme is energy-inefficient for resource-constrained IoT devices.

Figure 7 - Total energy consumption (Key generation / Cryptographic



Source: Authors

3.3 SUITABLE PKC SCHEMES FOR CONSTRAINED IOT DEVICES

To identify suitable PKC schemes for constrained IoT devices, several key factors must be considered: key distribution, security, and performance. All examined PKC schemes in this paper enable secure data exchange over insecure channels, providing confidentiality, non-repudiation, and authenticity. Unlike symmetric encryption, which relies on shared secret keys, PKC employs a public-

private key pair. The public key is shared, while the private key remains confidential. The mathematical relationship between these keys is computationally challenging to break, typically involving problems like the Discrete Logarithm Problem (DLP).

In terms of security, all studied PKC schemes offer a 128-bit security level, regardless of whether they are based on integer factorization (RSA, Rabin) or elliptic curves (ECIES, ECDSA, ECDH). However, a key distinction lies in cryptographic key size requirements. Elliptic curve schemes achieve 128-bit security with 256-bit keys, whereas integer factorization schemes necessitate significantly larger 3072-bit keys. This represents a notable disadvantage for RSA and Rabin schemes. Indeed, integer factorization schemes are less efficient than elliptic curve schemes due to their larger key sizes. This inefficiency manifests in higher memory consumption, increased microcontroller costs, and greater network bandwidth requirements. Therefore, RSA, and Rabin schemes are less suitable for practical in resource-constrained IoT environments.

Performance evaluations presented in Figures 6 and 7 indicate that ECIES, ECDSA, and ECDH consistently outperform RSA and Rabin in terms of computational efficiency and power consumption when executed on ARM microcontrollers. Accordingly, ECC-based schemes are deemed practical for deployment on resource-constrained IoT devices, including Arduino Zero, IoT LAB-M3, and Decawave DM1001 boards

4 CONCLUSION

This paper provides a comprehensive evaluation and analysis of various public-key cryptographic schemes on resource-constrained IoT devices, including IOTLAB-M3, Arduino-zero, and Decawave DWM1001. The study focused on comparing the performance of well-known public-key schemes in terms of computational time and energy consumption, highlighting the suitability of these schemes for resource-constrained environments. The results demonstrate that ECC-based schemes (ECIES, ECDSA, and ECDH) consistently outperform integer factorization-based schemes (RSA and Rabin) in terms of computational efficiency and power consumption. ECC schemes offer a significant advantage in

terms of key size, requiring significantly smaller keys to achieve the same level of security. This translates to reduced memory consumption, lower microcontroller costs, and less bandwidth requirements, making them more suitable for resource-constrained IoT applications. The study also highlights the energy inefficiency of the Rabin scheme, which significantly consumes more energy than other schemes due to its high computational cost. This makes the Rabin scheme less practical for resource-constrained IoT devices, where energy efficiency is crucial.

Overall, the paper concludes that ECC-based schemes are more suitable for deployment on resource-constrained IoT devices like Arduino Zero, IoT LAB-M3, and Decawave DM1001. This conclusion is based on the demonstrated performance advantages of ECC schemes in terms of computational efficiency, energy consumption, and key size requirements.

As a future work, IBAKAS will be extended with more research:

- Expand the Scope of Schemes and Platforms: Include a wider range of public-key schemes, including newer and more efficient algorithms like post-quantum cryptography schemes. Additionally, evaluate the performance on a larger and more diverse set of IoT platforms.
- Investigate other performance evaluation criteria: We will use additional performance evaluation criteria such as storage and communication costs.

REFERENCE

ADJIH, C., *et al*. (2015). Fit iot-lab: A large-scale open experimental IoT testbed. In 2015 ieee 2nd world forum on internet of things (wf-iot) (pp. 459–464).

AHMID, M., KAZAR, O., & BARKA, E. (2024). Internet of things overview: Architecture, technologies, application, and challenges. In Decision-making and security risk management for iot environments (pp. 1–19). Springer.

ARANHA, D. F., Gouvêa, C. P. L., Markmann, T., Wahby, R. S., & Liao, K. (2024). RELIC is an Efficient LIbrary for Cryptography. https://github.com/relic-toolkit/relic.

ARDUINO. (2024). Aduino zero board online specifications. [Online]. Available: https:// www.iot-lab.info/docs/boards/arduino-zero/. (Accessed August 2024).

BACCELLI, E., *et al*. (2018). Riot: An open source operating system for low-end embedded devices in the iot. IEEE Internet of Things Journal, 5 (6), 4428–4440.

BOUDIA, O. R. M., Senouci, S. M., & Feham, M. (2015). A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography. Ad Hoc Networks, 32, 98–113.

BROWN, D. (2009). Standards for efficient cryptography, sec 1: elliptic curve cryptography. Released Standard Version, 1.

DECAWAVE. (2024). DecaWave DWM1001 board online datasheet. [Online]. Available: https://www.decawave.com/dwm1001dev/schematic/. (Accessed August 2024).

FIT IOT-LAB. (2024). IoT-LAB M3 board online specifications. [Online]. Available: https://iot-lab.github.io/docs/boards/iot-lab-m3/. (Accessed August 2024).

GUBBI, J., BUYYA, R., MARUSIC, S., & PALANISWAMI, M. (2013). Internet of things (iot): A vision, architectural elements, and future directions. Future generation computer systems, 29 (7), 1645–1660.

HANKERSON, D., & MENEZES, A. (2021). Elliptic curve cryptography. In Encyclopedia of cryptography, security and privacy (pp. 1–2). Springer.
Mezrag, F., Bitam, S., & Mellouk, A. (2017). Secure routing in cluster-based wireless sensornetworks. In Globecom 2017-2017 ieee global communications conference (pp. 1–6).

MEZRAG, F., BITAM, S., & MELLOUK, A. (2019). Idsp: A new identity-based security protocol for cluster-based wireless sensor networks. In 2019 ieee 30th annual international symposium on personal, indoor and mobile radio communications (pimrc) (pp. 1–6).

MEZRAG, F., BITAM, S., & MELLOUK, A. (2022). An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor

networks. Journal of Network and Computer Applications, 200, 103282.

MURTHY, S., D'SOUZA, R. J., & VARAPRASAD, G. (2012). Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks. IEEE Sensors Journal, 12 (10), 2941–2949.

RABIN, M. O. (1979). Digitalized signatures and public-key functions as intractable as factorization.

RIVEST, R. L., SHAMIR, A., & ADLEMAN, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21 (2), 120–126.

VERMESAN, O., & FRIESS, P. (2013). Internet of things: converging technologies for smart environments and integrated ecosystems. River publishers.

ZHAO, S., AGGARWAL, A., FROST, R., & BAI, X. (2011). A survey of applications of identity-based cryptography in mobile ad-hoc networks. IEEE Communications surveys & tutorials, 14 (2), 380–400.