Faculté des Mathématiques et de l'Informatique

1985

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

University of Mohamed Boudiaf -M'sila

Faculty of Mathematics and Computer Sciences

Second National Conference on Mathematics and Applications

M'sila, Algeria - 27-28 Nov. 2024.

CERTIFICATE OF PARTICIPATION

The organizing committee of the Second National Conference on Mathematics and Applications, certifies that:

Fares Mezrag

Presented an **ORAL COMMUNICATION** entitled:

Implementation and Performance Evaluation of Public-Key Algorithms in Constrained Devices.

LMPA
Laboratoire de mathématiques pures et appliquées

Chairman of the NCMA'2024:
Pr. Noureddine BENHAMIDOUCHE

L.M.P.A

Implementation and Performance Evaluation of Public-Key Algorithms in Constrained Devices

Fares Mezrag [♭] and Noureddine Chikouche [♭]

(♭) LIAM Laboratory, University of M'sila
M'sila, Algeria.

Abstract

Designing efficient and lightweight cryptographic schemes is crucial for resource-constrained devices. This research paper evaluates the performance of five well-established public-key cryptographic schemes on three such devices: IOTLAB-M3, Arduino-Zero, and Decawave DWM1001. The evaluated schemes fall into two categories: integer factorization-based (RSA and Rabin) and elliptic curve-based (ECIES, ECDH, and ECDSA). Through comprehensive experiments, the paper compares the computational time and energy consumption of these schemes. The findings provide valuable insights for selecting the optimal cryptographic schemes to use in resource-limited environments.

Keywords: Security, public-key cryptography, constrained device, performance.

1 Introduction

To ensure the security of resource-constrained devices, it is essential to implement fundamental security measures, including authentication, data confidentiality, and data integrity. Additionally, the development of lightweight, efficient, and secure cryptographic schemes is crucial to accommodate the limitations of these devices.

Cryptographic techniques, such as Symmetric Key Cryptography (SKC) and Public Key Cryptography (PKC), can be employed to guarantee security properties like confidentiality, integrity, authentication, and non-repudiation. While SKC offers advantages in terms of computational efficiency and energy consumption, key distribution poses significant challenges. In contrast, PKC provides greater flexibility and simplifies key distribution, but it often incurs higher computational costs, which can be prohibitive for resource-constrained devices.

Recent research [4, 5] suggests that the application of PKC on resource-constrained devices is feasible. This paper aims to evaluate the performance of well-known public-key cryptographic schemes on three constrained devices: IOTLAB-M3, Arduino-zero, and DWM1001. Specifically, we assess the computational time and energy consumption associated with these schemes on the aforementioned devices.

2 Methods

This section explores various public-key algorithms and their development contexts.

2.1 Studied public-key algorithms

This paper analyzes a performance evaluation of five prominent public-key algorithms: RSA, Rabin, ECDH, ECIES, and ECDSA.

- **RSA algorithm:** RSA (Rivest–Shamir–Adleman) is an asymmetric cryptographic algorithm introduced by Rivest, Shamir, and Adleman [1]. Its security relies on the computational difficulty of factoring large integers. To achieve this, a massive integer, N, is employed to derive a public key (e) and a private key (d). Encryption is performed using the public key, while decryption necessitates the corresponding private key.

- **Rabin algorithm:** The Rabin cryptosystem is a public-key encryption algorithm proposed by Michael Rabin [2]. Its security is predicated on the computational intractability of integer factorization, a problem forming the foundation of numerous contemporary cryptographic systems. The algorithm's security is provably equivalent to the difficulty of factoring large integers.

- **ECDH algorithm:** Elliptic Curve Diffie-Hellman (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 $sk = k_A.Q_B = k_B.Q_A = k_A.k_B.G$.

- **ECIES algorithm:** Elliptic Curve Integrated Encryption 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 [3] for further details. Next, we demonstrate how to exchange a message using ECIES.

- **ECDSA algorithm:** Elliptic Curve Digital Signature Algorithm (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 QA to verify the authenticity of Alice's signature.

2.2 Implementation of public-key algorithms

We implemented the ECIES, ECDSA, ECDH, RSA, and Rabin cryptographic algorithms within the C programming language and the RIOT-OS [6], a lightweight operating system optimized for resource-constrained devices. Utilizing the RELIC toolkit [7], a suitable asymmetric cryptographic library for resource-constrained devices, we employed 3072-bit RSA/Rabin schemes and 256-bit Elliptic Curve Cryptography (ECC) schemes to achieve a 128-bit security level. The performance of the investigated public-key-based cryptographic algorithms was evaluated on three resource-constrained devices from the FIT IoT-LAB testbed [8]: the IOTLAB-M3, Arduino-zero, and DWM1001.

3 Results

To assess the performance of the studied algorithms, two key metrics were considered: computational cost and energy consumption.

3.1 Computational cost

The results, as depicted in Figure 1, indicate that the Rabin scheme incurs significantly higher computational costs compared to the other evaluated schemes. Consequently, the Rabin scheme is deemed computationally expensive and unsuitable for resource-constrained devices.

In contrast, the remaining schemes, as evidenced by the data presented in Figure 1, demonstrate suitability for deployment in resource-limited environments.

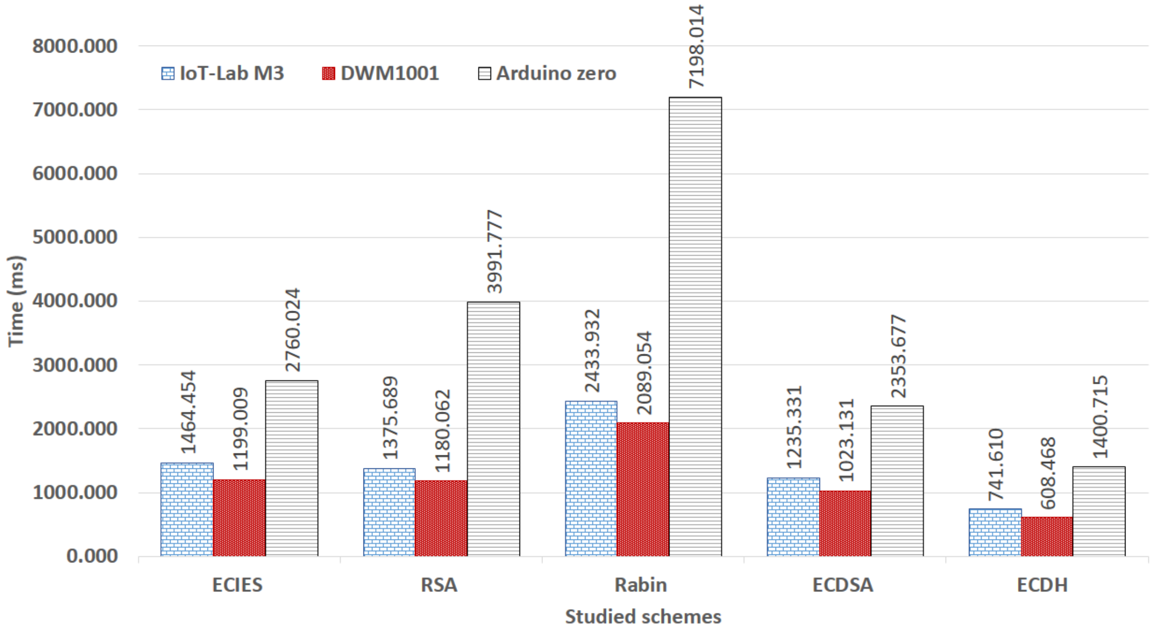

Figure 1: Computational cost of cryptographic operations.

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 millijoules (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 2 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 devices.

4 Conclusions

This paper presents a comprehensive evaluation and analysis of various public-key cryptographic schemes on resource-constrained devices, including the IOTLAB-M3, Arduino-zero, and Decawave DWM1001. The study focuses on comparing the performance of well-known public-key schemes in terms of computational time and energy consumption, with the aim of identifying suitable schemes for resource-constrained environments. The study also highlights the energy inefficiency of the Rabin scheme, which significantly consumes more energy than other schemes due to its high

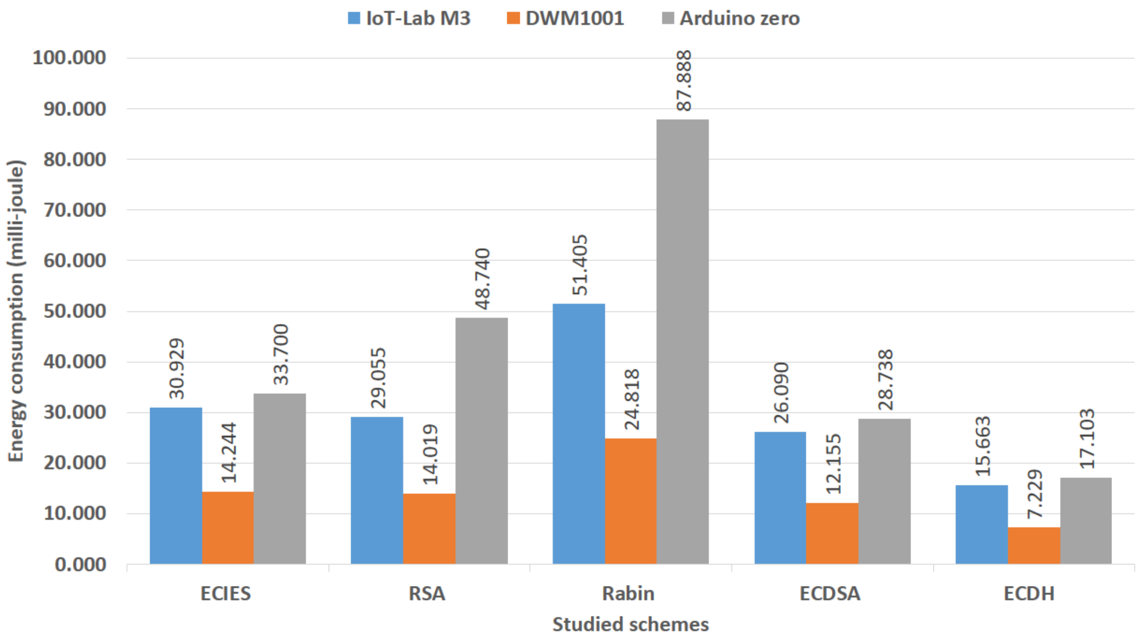

Figure 2: Total energy consumption (Key generation / Cryptographic operations.

computational cost. This renders the Rabin scheme less practical for resource-constrained devices, where energy efficiency is a critical consideration. Overall, the paper concludes that ECC-based schemes are more suitable for deployment on resource-constrained devices

References

[1] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.

[2] Rabin, Michael O. "Digitalized signatures and public-key functions as intractable as factorization." (1979).

[3] Brown, D. "Standards for efficient cryptography, SEC 1: elliptic curve cryptography." Released Standard Version 1 (2009).

[4] Zhao, Shushan, et al. "A survey of applications of identity-based cryptography in mobile ad-hoc networks." IEEE Communications surveys & tutorials 14.2 (2011): 380-400.

[5] Mezrag, Fares, Salim Bitam, and Abdelhamid Mellouk. "An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks." Journal of Network and Computer Applications 200 (2022): 103282.

[6] Baccelli, Emmanuel, et al. "RIOT: An open source operating system for low-end embedded devices in the IoT." IEEE Internet of Things Journal 5.6 (2018): 4428-4440.

[7] Aranha, Diego F. "RELIC is an Efficient LIbrary for Cryptography." http://code. google. com/p/relic-toolkit/ (2020).

[8] Adjih, Cedric, et al. "FIT IoT-LAB: A large scale open experimental IoT testbed." 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE, 2015.

Med Boudiaf University of Msila

Faculty of Mathematics and Informatics

Laboratory of Pures and Applied Mathematics

Second National Conference on Mathematics and Applications
M'sila, Algeria - 27-28 Nov. 2024

NCMA'2024 Program

About and Topics

About :

The second edition of the Conference on Mathematics and Applications serves as a platform for researchers and scientists, to exchange ideas and explore the latest advances in the field of mathematics and their applications. Our conference includes keynote speeches, paper presentations, and posters.

Topics :

- **Ordinary and Partial Differential Equations**
- **Algebra, Number theory, and applications**
- **Numerical Analysis and Applied mathematics: biology, image processing, fluid mechanics, ...**

First Day: Wednesday 27th November 2024

8h30 – 9h: Registration

9h – 9h 20: Opening Ceremony (Ibn El Haithem Conference Room)

Time	Plenary Session: (First Day : Wednesday 27th November 2024)
9h20-10h 45	**Chairman: Pr A. Medegheri - Dj. Bentorki**
9h20 – 10 h10	**Speaker**: Pr Lamnouar Noui Univ. Batna , Outils algébriques et applications.
10h10 – 10h 45	**Speaker**: Badreddine Benhellal - Univ. Oldenburg – Germany, On Schrödinger operators with oblique transmission conditions on non-smooth curve.
10h 45- 11h05	**Break Coffee**
11h 05-12 h30	**Chairman: Pr M. Hachama - A. Mansour**
11h 05 – 11h55	**Speaker**: Pr Nouri Fatma Zohra Univ. Annaba, A study of the dynamic of a fluid by an Atmospheric Pressure.
11h 55 – 12 h30	**Speaker**: Dr Bilel Selikh ENS- Bou Saada, Applications of non-commutative algebra in cryptography and security.
13h	**Lunch**

Oral parallel Sessions 1 (First Day : Wednesday 27th November 2024) - Afternoon		
Time	**Workshop 1:** Algebra, Number theory, and applications **Room 1** **Chairman**: Pr A. Boudaoud - L. Zedam	**Workshop 2:** fractional PDEs and ODEs **Room 2** **Chairman**: Pr Benyettou Benabderahmane - A. Yacine
14h – 14h 20	**Speaker**: Kheir Saadaoui, On a fuzzy lattice Instead to ,like computer sciences, chemistry	**Speaker**: Memou Ameur, An inverse source boundary value problem for a fractional parabolic differential equation of second order.
14h20 – 14h 40	**Speaker**: Hakim Moussaoui, Déformation in algebraic structures.	**Speaker**: Amouria Hamou, EXISTENCE RESULTS FOR FRACTIONAL DIFFERENTIAL INCLUSIONS.
14h40 – 15h 00	**Speaker**: Imane Douadi, Kinds of ideals and filters in hyperlattices semigroups.	**Speaker**: Ouagni Noura, Self-similar solutions of space-time fractional partial differential equation with Hilfer- Katugampola's Derivative.
15h – 15h 20	**Speaker**: Sylia Abdoun, A study on the impact information in Markovian queue with strategic customers.	**Speaker**: Bouthina Sabah Hammou, Existence and Uniqueness results for a Fractional Differential Equation with Integral Conditions
15h20 – 15h 40	**Coffee Break**	**Coffee Break**
15h40 – 16h 00	**Speaker**: Ahmed Benkahla, Construction of Bihom group	**Speaker**: Zakaria Malki, Combination of Hadamard derivative and boundary random fractional differential equations.
16h00 – 16h 20	**Speaker**: Oussama Zehani, Linearly multifunctions based construction of order relation.	**Speaker**: Imane Aouina, Analysis of a System of n-Nonlinear Fractional q-Differential Equations Involving Caputo

		q-Derivatives.
16h20 – 16h 40	**Speaker:** Adem Aikous, On the structure of ordered semi-hypergroup.	**Speaker**: Imane Boudrissa, A novel modification of the ROF model for image processing.
16h40 – 17h 00	**Speaker**: Saad Mohamed, Some properties of picture fuzzy subgroups on a group.	**Speaker**: Rami Amira, Chaos control in a fractional remanufacturing duopoly game.

Second Day : Thursday 28th November 2024

Oral parallel Sessions 2 (2nd day: Thursday 28th November 2024**)**		
Time	**Workshop 1:** Algebra, Number theory, and applications **Room 1** **Chairman**: D. Mihoubi - A. Amroune	**Workshop 2:** PDES and ODEs **Room 2** **Chairman**: Pr N. Bensalem - A. Gasmi
8h40 – 9h 00	**Speaker**: Heboob Lakhdar, Some cyclic codes of length 2p.	**Speaker**: Mimia Benhadri, Positive periodic solutions of of functional delay diferential equations with parameter.
9h00 – 9h 20	**Speaker**: Fares Mezrag, Implementation and Performance Evaluation of Public-Key Algorithms in Constrained Devices.	**Speaker**: Houd Kheireddine, Analysis of frictionless contact problem with friction.
9h20 – 9h 40	**Speaker**: Zahra Amroune, On factoring of unlimited generalized Fibonacci numbers.	**Speaker**: Haroune Lamrad, On The existence of the solution to an elliptic non-local problem involving critical Sobolev exponent.
9h40 – 10h 00	**Speaker**: Nasser Ghedbane, New Public Key Cryptosystem Using the Isomorphism Problem on Matrix Representations of finite Groups.	**Speaker**: Chahnaz Zakia Timimoun, Stability of the nonlinear Korteweg-de Vries equation.
10h00 – 11h 00	**Coffee Break and Poster Session**	
11h00 – 11h 20	**Speaker**: Frahtia Nassim, Localization of some functional spaces.	**Speaker**: Abdelaziz Hellal, REGULARIZING EFFECT IN SOME ANISOTROPIC NONLINEAR DIRICHLET PROBLEM.
11h20 – 11h 40	**Speaker**: Sara Boudaoud, A study on fuzzy graphs.	**Speaker**: Meriem Araour, NEW RESULTS FOR SOLVING LOGARITHMIC FUZZYINTEGRO-DIFFERENTIAL EQUATION:EXISTENCEAND UNIQUENESS OF THE SOLUTION
12h00 – 12h 20	**Speaker**: Ahlem Hamani, Some Properties Of Minimal Non-Finite-By-(Locally Nilpotent) Groups.	**Speaker**: H. Ait Mohammed, Existence and uniqueness results of solutions for a multi-point Riemann-Liouville fractional boundary value problem (RL-FBVP).

	Speaker: Rachid Chergui, La théorie du codage sur l'extension des nombres de Lucas.	**Speaker**: Bilel Madjour, Asymptotic behavior of memory-type thermoelastic problem with a polynomial source.
12h30	**Closing and Lunch**	**Closing and Lunch**

Oral parallel Sessions 2 (2nd day: Thursday 28th November 2024**)**		
Time	**Workshop 3:** Algebra, Number theory, and applications **Room 3** **Chairman** F.Z. Nouri - A. Merzougui	
8h40 – 9h 00	**Speaker**: Amina Khirani, Lucas Collocation Method for Solving linear Fredholm Integral Equations of the second kind.	
9h00 – 9h 20	**Speaker**: Abdelouahab Mani, A Comparative Study of Numerical Methods for Solving Integral Delay Equations.	
9h20 – 9h 40	**Speaker**: Bounouiga Souad, Mathematical Modeling of Malaria Transmission: Analysis and Numerical Simulation.	
9h40 – 10h 00	**Speaker**: Bochra Amroune, Application of the Hilbert method to the analysis of free surface flow phenomena.	
10h00 – 11h 00	**Coffee Break and Poster Session**	
11h00 – 11h 20	**Speaker**: Chouder Rafaa, Fast difference scheme for a general mean curvature Flow.	
11h20 – 11h 40	**Speaker**: Lachache Mohamed, Theoretical and Numerical results for a shallow water model coupled with a transport equation.	
11h 40– 12h 00	**Speaker**: Hemici Youcef Elhamam, Study of a diagonalconjugate gradient-like method using different line searches.	
12h00 – 12h 20	**Speaker**: Hossemddine Achour, Self-similar solutions for free boundary problem and contour enhancement in image.	
12h30	**Closing and Lunch**	

Poster Session1 (2nd day: Thursday 28th November 2024)
10h00 – 11h 00

P1 : Bounab Noura , Two-dimensional Potential Flow through a Nozzle.
P2 : Nadir Hana, Existence results for nonlinear problems when the source term is small.
P3 : Saqd Abdelkebir, Approximate Solution for Time-Conformable Fractional Heat Equations Using Adomian Decomposition Method.
P4 : Khayra Djerioui, coefficient problem for a time-fractional diffusion-wave equation with nonlocal boundary conditions.
P5 : Barkahoum Chebabhi, Shifted fifth-kind Chebyshev spectral approach for solving Volterra-Fredholm integro differential Equations.
P6 : Fatma seraiche, SUPERCONVERGENCE OF THE ITERATED GALERKIN METHOD FOR INTEGRAL EQUATIONS OF THE SECOND KIND.
P7 : Abderrazak Mehllou, numerical solution of fredholm integral equations using galerkin-legendre-wavelets method.
P8 : Lamine Salaheddine, An inverse problem for a time-fractional reaction-diffusion equation with involution and periodic boundary conditions.
P9 : Nour el imane Khadidja CHERIET, The hyper order and fixed points of solutions of a class of linear differential equations.
P10 : Chahinez Chhi ; Existence and uniqueness of positive solution for some nonlocal elliptic problem.
P11 : HIBATERRAHMANE BENMESSAOUD , PROPERTY OF LAMINAR FLOW OF BINGHAM FLUID.
P12 : Benaissi Brahim , THE FUNDAMENTAL EXISTENCE OF A SOLUTION TO THE GENERALIZED LINEAR FRACTIONAL DIFFUSION EQUATIO.
P13 : Aissa Amour, Numerical simulation of cement particle dispersion in a Cement-Mill Fan for erosion prediction.

N.B : It is preferred to present posters in A0 format