THE INTERNATIONAL SYMPOSIUM ON INNOVATIVE INFORMATICS OF BISKRA

CERTIFICATE OF ATTENDANCE

This is to certify that

Anwar Noureddine BAHACHE

has presented the paper entitled

"An Efficient ECC-Based Authentication Protocol for Secure RFID Healthcare Applications"

during the **IEEE International Symposium on iNnovative Informatics of Biskra (ISNIB'2025)**

held at Mohamed Khider University, Biskra, Algeria, January 28–30, 2025.

Program Chair

Program Chair
Prof. Laid KAHLOUL

The International Symposium on iNnovative Informatics of Biskra'2025 (ISNIB'25)

Organization Chair

رئيس قسم الإعلام الآلي
بن دحمان توفيق

MOHAMED KHIDER UNIVERSITY OF BISKRA
FACULTY OF EXACT, NATURAL AND LIF SCIENCES
COMPUTER SCIENCE DEPARTEMENT

LRP · IEEE Algeria Section · IEEE Xplore Digital Library

An Efficient ECC-Based Authentication Protocol for Secure RFID Healthcare Applications

Anwar Noureddine Bahache
National Higher School of Mathematics (NHSM)
Algies, Algeria

Noureddine Chikouche
LIAM Laboratory
University of M'sila
M'sila, Algeria

Mohamed Bahache
LIAM Laboratory
University of M'sila
M'sila, Algeria

Fares Mezrag
LIAM Laboratory
University of M'sila
M'sila, Algeria

***Abstract*—As Internet and Communication Technologies (ICT) evolve, RFID (Radio Frequency Identification) has become essential in healthcare for efficiently tracking and managing tagged medical devices. While RFID tags are extensively used on various healthcare assets, they are exposed to serious security and privacy risks, such as eavesdropping, data tampering, and interception, which threaten the confidentiality of healthcare professionals and patients. Despite the development of multiple lightweight RFID authentication schemes, many still suffer from vulnerabilities like replay, impersonation, and de-synchronization attacks. To address these limitations, we present a robust and efficient RFID authentication scheme designed specifically for IoT-enabled healthcare applications. By integrating Elliptic Curve Cryptography (ECC), our scheme delivers strong security with a low computational footprint, ensuring resilience against all evaluated attack types. Comprehensive security and performance testing demonstrate that our protocol offers an effective balance of security and efficiency, making it an ideal and secure choice for real-time healthcare environments.**

***Index Terms*—RFID systems, authentication protocols, healthcare applications, Elliptic curve cryptography, security**

I. Introduction

With rapid progress in ICT and automated medication systems, RFID and WBAN technologies are increasingly integrated into healthcare to improve patient safety [1], [2]. As a fundamental tool in pervasive computing, RFID allows for the unique, simultaneous identification of multiple items over a shared channel. RFID applications span a wide range, including automated payments, access control, toll systems, personnel tracking, e-healthcare, and supply chain management [3].

In healthcare, RFID brings advantages such as theft prevention, decreased human error, increased productivity, and cost savings. Emerging smart healthcare systems utilize RFID for continuous monitoring, mobility, and remote access to patient data through cloud-based servers. While patient misidentification remains a challenge, RFID helps mitigate such risks by supporting precise asset and patient tracking, enhancing safety, and improving operational efficiency. Despite these benefits, concerns over security, privacy, and safety continue to limit broader adoption [4], [5].

Our contribution is an ECC-based RFID authentication scheme specifically designed for healthcare systems, effectively safeguarding patient data and medical records over vulnerable wireless channels between tags (e.g., patients) and readers (e.g., medical staff). Unlike secure channels used between readers and servers, the wireless connection between tags and readers remains exposed, requiring a strong RFID authentication solution. The primary goals of our protocol include:

- Establishing mutual authentication among the tag, reader, and server.
- Ensuring compliance with security requirements for RFID healthcare systems.
- Providing resilience against known security attacks.
- Achieving lower computational and storage costs for resource-constrained environments.

Our ECC-based scheme not only enhances security but also maintains efficiency, offering a practical solution for secure, real-time healthcare applications.

The remainder of our paper is organized as follows: Section II presents existing related works in literature. In Section III we present our system model and detail the different steps of the proposed protocol. In Section IV a security analysis is presented followed by a performance analysis in SectionV, with a discussion. Finally, our manuscript is concluded in Section VI.

II. Related work

In recent years, various RFID authentication schemes have been introduced to secure RFID systems against diverse security threats. Low-cost RFID systems face challenges in ensuring complete security and privacy due to insecure communication between tags and readers. To address these issues, we review previous schemes along with their cryptographic methods, strengths, and weaknesses.

Noori et al. [6] presented a scalable, efficient ECC and hash-based protocol for healthcare, allowing low-cost addition or revocation of devices and focusing on secure, scalable RFID communication.

Zhu Feng [7] critiqued Safkhani and Vasilakos's protocol [8] and proposed a secure RFID protocol based on hash and square root operations. Although effective in privacy, its high resource demand highlights a trade-off between security and performance. Xie et al. [9] addressed back-end server vulnerabilities in RFID by incorporating an indistinguishability obfuscation technique. Extending to cloud storage, they reduced on-device costs and mitigated data leakage risks associated with traditional servers. Salem et Amin [10] designed a privacy-preserving protocol for Telecare Medicine Information Systems (TMIS) using El-Gamal cryptography to safeguard patient safety.

Lately, Agrahari and Varma [11] applied ECC-based Qu-Vanstone certificates for mobile, secure, and scalable healthcare authentication with minimal computation and key size requirements. Izza et al. [12] proposed an ECC and ECDSMR-based RFID protocol to improve Naeem et al. [13] scheme for wearable healthcare networks (WBANs), focusing on strengthened security over the internet.

Song et al. [14] introduced ZKAP, a zero-knowledge RFID authentication protocol, offering strong privacy features but lacking formal security verification. Shariq and Singh [15] recently proposed a lightweight RFID-enabled protocol for healthcare, leveraging vector space properties to enhance security and efficiency. However, it was found to be vulnerable to tag anonymity and impersonation attacks [16]. Kumar et al. [17] introduced a privacy-preserving, lightweight mutual authentication and session key generation scheme aimed at establishing secure communication for RFID-enabled IoMT devices.

III. Proposed Protocol

Our proposed protocol includes two primary phases: Initialization and Registration, which may be further split, and Authentication.

A. System model

The proposed RFID-based healthcare system architecture consists of several key components: RFID tags, an RFID reader, and a Trusted Authority (TA) responsible for registrations and management of the system.

- **RFID Tags:** Each patient or healthcare entity is assigned an RFID tag that contains unique identification information. These tags can store various types of data, including patient medical history, allergies, medications, and other relevant health information.
- **RFID Reader:** The RFID reader is a device that emits radio waves to communicate with RFID tags. It can read and write data to the tags within its range. In the healthcare system, the reader is typically placed at strategic locations to facilitate the quick retrieval of patient information.
- **Trusted Authority** (TA)**:** The Trusted Authority is responsible for managing the registration and authentication processes within the RFID-based healthcare system. It ensures that only authorized personnel can access sensitive patient information.

The operation of our RFID-based healthcare system can be described as follows:

1) **Registration:** When a new patient is admitted, the TA registers the patient in the system. This process involves issuing a unique RFID tag to the patient and storing their relevant information in the secure database.

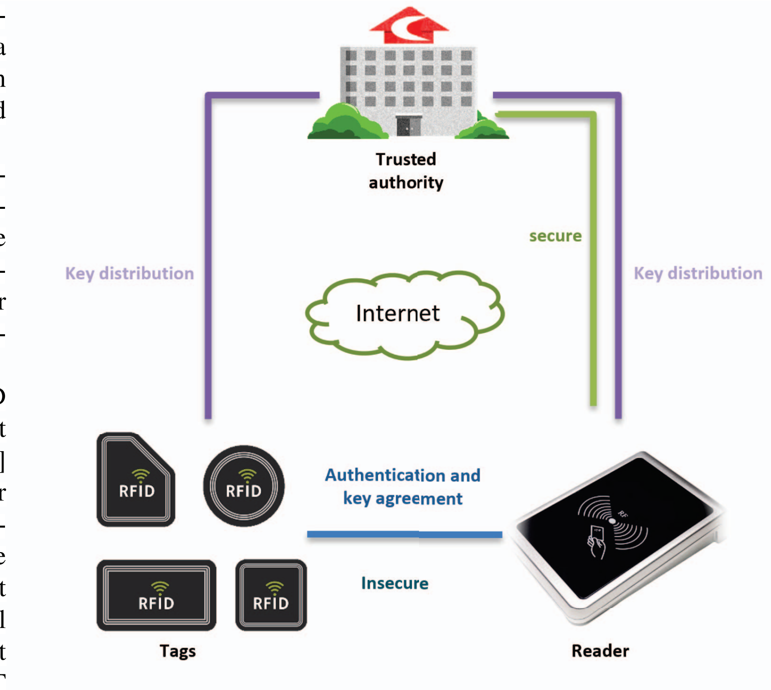

Fig. 1. RFID system for healthcare application.

2) **Data Retrieval:** When a healthcare professional needs to access a patient's information, they use the RFID reader to scan the patient's RFID tag which represents a direct communication to the TA. The reader retrieves the associated data from the TA's database, allowing for quick and efficient access to the patient's medical history.
3) **Access Control:** The TA enforces strict access control policies to ensure that only authorized personnel can access sensitive data. This includes authentication mechanisms to verify the identity of healthcare professionals before granting access to patient information.
4) **Data Security:** To protect patient information from unauthorized access and ensure data integrity, the system employs various security measures, including ECC, hash, secure communication protocols, and regular security audits.

Figure 1 represents our basic RFID architecture model.

B. Enhanced Key Generation Scheme with Increased Resilience to Adversaries

- **Initialization by Trusted Authority (TA)**:
  - The TA selects an elliptic curve E_q over the finite field F_q, where q is a prime number, and a base point P of order n on E_q.
  - TA generates its private key $\alpha \in [1, n-1]$ and computes the public key:

$$TA_{pk} = \alpha \cdot P \tag{1}$$

  - TA computes a salted hash $H_s(\alpha) = H(\alpha||s)$, where s is a securely generated salt, which will be used to obscure α further in later computations.
- **Entity U_v Key Component Generation with Hash-Based Masking**:
  - Each entity U_v selects a random integer $c_v \in [1, n-1]$.
  - U_v computes a masked value for d_v using a blinding factor and hash-based masking:

$$d_v = H(c_v||r_v) \cdot P \quad (2)$$

    Where r_v is a randomly chosen nonce. This prevents an adversary from deducing c_v from d_v.
  - U_v sends $(d_v, H(ID_v||r_v))$ to the TA, where $H(ID_v||r_v)$ is a hash of U_v's ID concatenated with r_v, adding session-specific randomness to protect ID_v.
- **Trusted Authority's Enhanced Computation for Entity U_v**:
  - The TA selects a random integer $w_v \in [1, n-1]$ and computes a session-based "blinded" intermediate point:

$$y_v = (w_v \cdot P) + H(d_v||s) \cdot P \quad (3)$$

    Here, $H(d_v||s)$ introduces an additional level of obscurity with salt s, making it difficult to reverse engineer d_v from y_v.
  - TA computes z_v by including both $H_s(\alpha)$ and the hashed identifier $H(ID_v||r_v)$:

$$z_v = w_v + ((y_v)_x + H(ID_v||r_v)) \cdot H_s(\alpha) \mod n \quad (4)$$

  - TA sends (y_v, z_v) to U_v.
- **Entity U_v's Final Secret Key Calculation with Multi-layer Hashing and Verification**:
  - U_v computes its private key x_v by combining z_v, c_v, and the session nonce r_v:

$$x_v = (z_v + H(c_v||r_v)) \mod n \quad (5)$$

  - U_v verifies its key x_v using multi-factor verification:

$$x_v \cdot P = y_v + ((y_v)_x + H(ID_v||r_v)) \cdot TA_{pk} \quad (6)$$

    Here, $H(ID_v||r_v)$ further binds the identity and session randomness, ensuring that even if some elements are exposed, they cannot be easily correlated or reused by an adversary.

C. Authentication phase

This scheme provides mutual authentication between a reader U_R and a tag U_S by incorporating random values and timestamps to ensure session uniqueness and prevent replay attacks.

- **Initialization by TA and Shared Information:**
  - The elliptic curve E_q, base point P, and the public key of TA, TA_{pk}, are known to both U_R and U_S.
  - Both entities (reader U_R and tag U_S) have unique identifiers ID_R and ID_S, as well as pre-shared hashed identifiers $H(ID_R)$ and $H(ID_S)$ with the TA.
- **Mutual Authentication Protocol:**
  - **Step 1:** U_R Initiates Authentication.
    * U_R selects:
      · A random nonce $r_R \in [1, n-1]$,
      · A random ephemeral value R_R for added security,
      · And generates a current timestamp T_R.
    * U_R computes the initial message for U_S:

$$M_1 = x_R \cdot H(ID_R||r_R||R_R||T_R) \cdot P \quad (7)$$

    * U_R sends $(M_1, y_R, ID_R, H(r_R||R_R), T_R)$ to U_S.
  - **Step 2:** U_S Verifies U_R and responds.
    * U_S checks that the timestamp T_R is within an acceptable range to ensure freshness.
    * U_S verifies M_1 by checking:

$$M_1 = x_R \cdot H(ID_R||r_R||R_R||T_R) \cdot P \quad (8)$$

      If verification is successful, U_S proceeds with the response.
    * U_S then selects:
      · A random nonce $r_S \in [1, n-1]$,
      · An ephemeral random value R_S,
      · And generates a current timestamp T_S.
    * U_S computes its response message:

$$M_2 = x_S \cdot H(ID_S||r_S||R_S||T_S) \cdot P \quad (9)$$

    * U_S calculates a session key K_{RS}:

$$K_{RS} = H(x_S \cdot y_R||r_R||r_S||R_R||R_S||T_R||T_S) \quad (10)$$

    * U_S sends $(M_2, y_S, ID_S, H(r_S||R_S), T_S)$ to U_R.
  - **Step 3:** U_R Verifies U_S and completes Authentication.
    * U_R checks that the timestamp T_S is within an acceptable range for the freshness of the message.
    * U_R verifies M_2 by checking:

$$M_2 = x_S \cdot H(ID_S||r_S||R_S||T_S) \cdot P \quad (11)$$

      If the calculated M_2 matches that sent by U_S, U_R confirms the authenticity of U_S.
    * U_R computes the session key K_{RS} independently:

$$K_{RS} = H(x_R \cdot y_S||r_R||r_S||R_R||R_S||T_R||T_S) \quad (12)$$

- **Final Session Key and Secure Communication:**
  - Both U_R and U_S now share the same session key K_{RS}, which is used for encrypted communication.
  - To secure each exchanged message, U_R and U_S use symmetric encryption with K_{RS} as encryption key.
  - Each message is prefixed with an MAC derived from K_{RS}, which ensures data integrity.

Figure 2 summarizes the authentication process.

Reader U_R — Tag U_S

Step 1: Initiate Authentication

Select r_R, R_R, and T_R
$M_1 = x_R \cdot H(ID_R \parallel r_R \parallel R_R \parallel T_R) \cdot P$
Sends $(M_1, y_R, ID_R, H(r_R \parallel R_R), T_R)$

$\longrightarrow$

Step 2: Verify and Respond

Verify M_1 and T_R
Select r_S, R_S, and T_S
$M_2 = x_S \cdot H(ID_S \parallel r_S \parallel R_S \parallel T_S) \cdot P$
$K_{RS} = H(x_S \cdot y_R \parallel r_R \parallel r_S \parallel R_R \parallel R_S \parallel T_R \parallel T_S)$
Sends $(M_2, y_S, ID_S, H(r_S \parallel R_S), T_S)$

$\longleftarrow$

Step 3: Verify Response

Verify M_2 and T_S
Derive $K_{RS} = H(x_R \cdot y_S \parallel r_R \parallel r_S \parallel R_R \parallel R_S \parallel T_R \parallel T_S)$
Calculate matching K_{RS} and starts the session

$\longrightarrow$

Both U_R and U_S now share K_{RS} for secure communication.

Fig. 2. Authentication process of the proposed protocol

IV. Security analysis

In this section, we assess the security of the proposed protocol using the robust Dolev–Yao (DY) threat model [18], which permits attackers to intercept, alter, and replay messages transmitted over a public network channel. Additionally, we present a comparison of our protocol with existing authentication protocols, highlighting security features (see Table I).

This analysis summarizes the defense mechanisms of the protocol against various security threats.

1) **Replay Attack Resistance**
   - The protocol uses timestamps T_R and T_S, ensuring messages are fresh. Each entity checks the timestamp to confirm it is within an acceptable range.
   - Random values r_R, r_S and ephemeral values R_R, R_S make each session unique, preventing reuse of old messages.
2) **Man-in-the-Middle (MitM) Attack Resistance**
   - ECC-based key generation and message validation ensure that only someone with legitimate private keys can authenticate.
   - The session key K_{RS} requires knowledge of multiple parameters (private keys, IDs, random values, timestamps), making it infeasible for an adversary to compute without access to all inputs.
3) **Impersonation Attack Resistance**
   - Mutual authentication is achieved by verifying computed messages M_1 and M_2 alongside timestamps and random values.
   - Hashing of IDs ensures only legitimate parties with correct private keys can generate valid responses.
4) **Session Key Freshness and Independence**
   - The session key K_{RS} is derived from both private keys x_R and x_S, along with unique session parameters (nonces, ephemeral values, timestamps), ensuring uniqueness for each session.
   - Even if a previous session key is compromised, it cannot be reused in future sessions due to the unique values generated each time.
5) **Resistance to Key Compromise Impersonation (KCI) Attacks**
   - Deriving K_{RS} from both private keys and unique session parameters prevents an adversary with access to one private key from impersonating the other party.
   - ECC-based mutual authentication ensures that key compromise does not lead to full protocol compromise.
6) **Forward Secrecy**
   - Unique random values and timestamps ensure forward secrecy; compromising x_R or x_S in the future does not allow reconstruction of past session keys.
7) **Resistance to Known-Key Attacks**
   - Each session key K_{RS} is independent due to the use of ECC-derived keys, random values, and unique timestamps. Previous session keys do not aid in deriving future keys.
8) **Data Integrity and Confidentiality**
   - A Message Authentication Code (MAC) derived from K_{RS} ensures message integrity. Unauthorized modifications lead to MAC verification failure.
   - Symmetric encryption (e.g., AES) with K_{RS} guarantees confidentiality, making messages readable only by the parties who share K_{RS}.

The comparison (see Table I) reveals that most protocols do not fully satisfy all essential security and privacy requirements. However, our proposed protocol not only meets all these requirements but also resists every discussed attack, ensuring robust protection across all fronts. This makes our protocol a superior choice for secure, resilient RFID authentication in vulnerable environments.

TABLE I
Different security requirements and attacks in the studied protocols

Protocol	A1	A2	A3	A4	A5	A6	A7
[6]	✓	✓	∗	✓	∗	∗	✓
[7]	✓	✓	✓	✓	∗	✓	∗
[10]	✓	✓	✓	✓	✓	✓	✓
[11]	✓	∗	✓	✓	∗	∗	✓
[12]	×	×	×	✓	∗	×	✓
Our	✓	✓	✓	✓	✓	✓	✓

✓: Ensure/Resist ×: Fails to ensure/resist ∗ : not discussed
A1: Anonymity A2: Forward/Backward secrecy
A3: Untraceability A4: Replay attack A5: DoS attack
A6: Desynchronization attack A7: Impersonation attack

TABLE II
PERFORMANCE EVALUATION OF THE STUDIED PROTOCOLS

Protocol	Computational cost	Communication cost	Storage cost
[6]	$T_{ECM} + 2T_H + 2T_S$	$4L_B$	$L_{ECM} + 4L$
[7]	$3T_H + T_{MODS}$	$9L + 3L_B$	$2L_B$
[10]	$3T_H + 2T_{MODS} + T_{MULT}$	$3L + 2L_B$	$3L + L_B$
[11]	$2T_{ECM} + T_{ECA} + 2T_H + 3T_{MULT}$	$2L_{ECM} + L_{ID} + 2L$	$L_{ECM} + 6L + L_{ID}$
[12]	$3T_{ECM} + 6T_H + T_S$	$6L + 3L_{ECM} + 5L_{TS}$	$L_{ID} + 2L + 3L_{ECM} + L_B$
Our	$2T_{ECM} + 3T_H$	$5L + 2L_{TS}$	$2L_{ECM} + L_{ID}$

V. PERFORMANCE ANALYSIS

We employed the RELIC Toolkit [19] for implementing both symmetric and asymmetric cryptographic operations, leveraging its lightweight, efficient framework for asymmetric algorithms. The experimental setup was hosted on the FIT IoT-LAB: Open Experimental IoT Testbed [20], [21], which includes a wide range of low-power wireless nodes and mobile robots, enabling large-scale IoT testing. Our implementation was run on an ST B-L475E-IOT01A board, which features a 64-Mbit Quad-SPI (Macronix) Flash memory, an Arm Cortex-M4 core with 1 Mbyte of Flash memory, and 128 Kbytes of SRAM.

Table III outlines the cryptographic primitives used across the frameworks we analyzed, along with the respective computational times and energy consumption observed in our implementation. Also, table IV presents the communication cost assumptions.

Figure 3 presents the computational, communication, and storage costs for the studied protocols on the tag side. Below, we analyze the performance based on these metrics.

- **Computational Cost**: Among existing schemes, Noori et al. [6] achieves the lowest computational cost at 261.95 ms due to the use of low-cost crypto-primitives. In contrast, protocols like Salem et al. [10] and Agrahari et al. [11] require significantly higher times (1205.526 ms and 870.72 ms, respectively) due to the intensive use of ECC and quadratic residue operations. Our proposed protocol offers a balanced alternative, requiring only 522.594 ms while maintaining strong security without the computational strain of extensive ECC operations.
- **Communication Cost**: Protocols such as Salem et al. [10] and Agrahari et al. [11] maintain lower communication costs of 352 bytes, whereas Zhu et al. [7] incurs up to 672 bytes. Our protocol achieves a further reduction, with only 168 bytes, offering efficient communication while preserving security standards.
- **Storage Cost**: For storage, Xie et al. [10] uses just 224 bytes, making it suitable for RFID systems with limited memory. Our protocol improves on this with a minimal storage requirement of only 96 bytes, making it ideal for RFID systems with strict memory constraints.

In summary, even though Noori et al. [6] manage to be the most efficient in terms of computation it still fails to protect against various attacks and doesn't provide all security and privacy requirements. On the other hand, our protocol balances security and efficiency by reducing computational, communication, and storage costs. This positions it as a highly practical solution for RFID applications in resource-constrained environments.

TABLE III
PERFORMANCE OF IMPLEMENTATION OF CRYPTOGRAPHIC PRIMITIVES

Operation	Notation	Timing (in ms)
Hash function/RNG (SHA-256)	T_H	0.154
Symmetric Enc/Decryption (AES-128)	T_S	0.288
Scalar point multiplication (Curve BN-P254)	T_{ECM}	261.066
ECC Addition (Curve BN-P254)	T_{ECA}	197.68
Modular operation	T_{MOD}	520.432
Modular square/exponentiation operation	T_{MODS}	577.432
Modular multiplication	T_{MULT}	50.2

TABLE IV
ASSUMPTIONS FOR COMMUNICATION COST CALCULATION

Notation	Description	Value
L_{ID}	Length of ID	32 bytes
L	Length of hash function result and symmetric key	32 bytes
L_{ECM}	Length of ECC point	128 bytes
L_{TS}	Length of timestamp	4 bytes
L_B	Length of large numbers and modulus operation result	128 bytes

VI. CONCLUSION

In this research, we introduced an advanced lightweight RFID authentication scheme tailored for IoT-enabled healthcare environments, addressing core security and privacy challenges in tracking medical assets. Leveraging Elliptic Curve Cryptography (ECC), our protocol offers a strong security foundation with low computational and storage requirements, making it well-suited for resource-limited RFID tags. Comprehensive security analysis showed that our protocol effectively mitigates attacks such as replay, impersonation, and desynchronization, outperforming many existing schemes vulnerable to these threats.

Performance evaluations confirmed the protocol's efficiency, underlining its practical applicability for real-time healthcare scenarios. This balance of robust security with minimal resource demands positions our scheme as a viable and secure choice for healthcare systems where data privacy and operational reliability are essential.

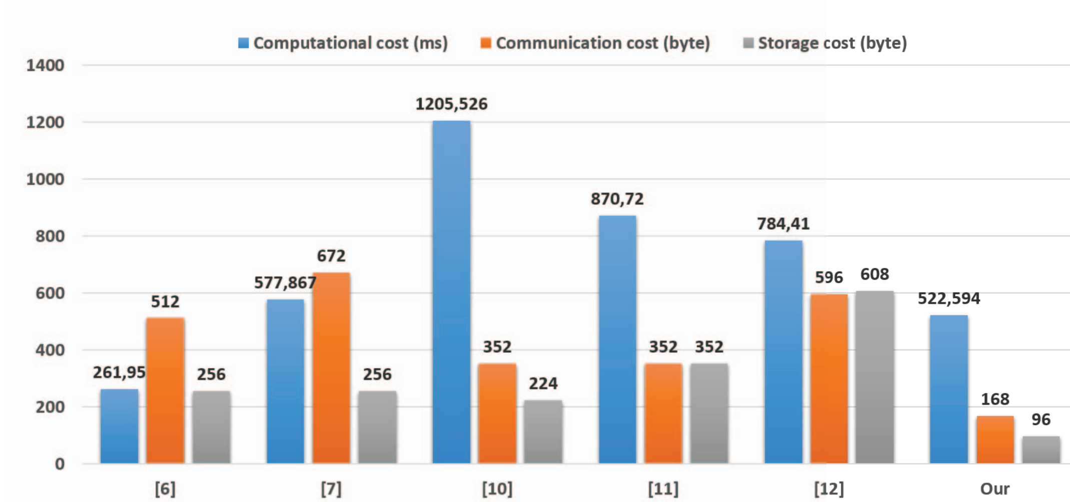

Fig. 3. Costs of the related protocols and the proposed protocol

Future work will consider verifying the proposed protocol using one of the well-known tools such as AVISPA and expanding the scheme's adaptability to evolving RFID standards and optimizing its performance for large-scale implementations, reinforcing its value in safeguarding IoT-driven healthcare applications.

References

[1] A. N. Bahache, N. Chikouche, and F. Mezrag, "Authentication schemes for healthcare applications using wireless medical sensor networks: A survey," *SN Computer Science*, vol. 3, no. 5, p. 382, 2022.

[2] A. N. Bahache, N. Chikouche, and S. Akleylek, "Securing cloud-based healthcare applications with a quantum-resistant authentication and key agreement framework," *Internet of Things*, vol. 26, p. 101200, 2024.

[3] N. Dinarvand and H. Barati, "An efficient and secure rfid authentication protocol using elliptic curve cryptography," *Wireless Networks*, vol. 25, no. 1, pp. 415–428, 2019.

[4] W. Yao, C.-H. Chu, and Z. Li, "The use of rfid in healthcare: Benefits and barriers," in *2010 IEEE International Conference on RFID-Technology and Applications*. IEEE, 2010, pp. 128–134.

[5] A. N. Bahache and N. Chikouche, "A comparative analysis of rfid authentication protocols for healthcare applications," in *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*. IEEE, 2021, pp. 1–6.

[6] D. Noori, H. Shakeri, and M. N. Torshiz, "Scalable, efficient, and secure rfid with elliptic curve cryptosystem for internet of things in healthcare environment," *EURASIP Journal on Information Security*, vol. 2020, no. 1, pp. 1–11, 2020.

[7] F. Zhu, "Secmap: a secure rfid mutual authentication protocol for healthcare systems," *IEEE Access*, vol. 8, pp. 192 192–192 205, 2020.

[8] M. Safkhani and A. Vasilakos, "A new secure authentication protocol for telecare medicine information system and smart campus," *IEEE Access*, vol. 7, pp. 23 514–23 526, 2019.

[9] S. Xie, F. Zhang, and R. Cheng, "Security enhanced rfid authentication protocols for healthcare environment," *Wireless Personal Communications*, vol. 117, no. 1, pp. 71–86, 2021.

[10] F. M. Salem and R. Amin, "A privacy-preserving rfid authentication protocol based on el-gamal cryptosystem for secure tmis," *Information Sciences*, vol. 527, pp. 382–393, 2020.

[11] A. K. Agrahari and S. Varma, "A provably secure rfid authentication protocol based on ecqv for the medical internet of things," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1277–1289, 2021.

[12] S. Izza, M. Benssalah, and K. Drouiche, "An enhanced scalable and secure rfid authentication protocol for wban within an iot environment," *Journal of Information Security and Applications*, vol. 58, p. 102705, 2021.

[13] M. Naeem, S. A. Chaudhry, K. Mahmood, M. Karuppiah, and S. Kumari, "A scalable and secure rfid mutual authentication protocol using ecc for internet of things," *International Journal of Communication Systems*, vol. 33, no. 13, p. e3906, 2020.

[14] J. Song, P.-W. Harn, K. Sakai, M.-T. Sun, and W.-S. Ku, "An rfid zero-knowledge authentication protocol based on quadratic residues," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12 813–12 824, 2021.

[15] M. Shariq and K. Singh, "A secure and lightweight rfid-enabled protocol for iot healthcare environment: A vector space based approach," *Wireless Personal Communications*, vol. 127, no. 4, pp. 3467–3491, 2022.

[16] H. Ghosh, P. K. Maurya, and S. Bagchi, "Cryptanalysis of an rfid-enabled authentication protocol for healthcare," *Wireless Personal Communications*, pp. 1–23, 2024.

[17] V. Kumar and S. K. Das, "A light weight mutual authentication and key generation scheme for rfid systems used in medical iot," in *2024 IEEE 3rd International Conference on Control, Instrumentation, Energy & Communication (CIEC)*, 2024, pp. 49–54.

[18] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[19] D. F. Aranha and C. P. Gouvêa, "RELIC is an Efficient LIbrary for Cryptography," 2020. [Online]. Available: https://github.com/relic-toolkit/relic

[20] C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele *et al.*, "Fit iot-lab: A large scale open experimental iot testbed," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 2015, pp. 459–464.

[21] A. N. Bahache, N. Chikouche, M. Bahache, and F. Mezrag, "A new authentication protocol for rfid-based healthcare application," in *The Sixth International Symposium on Informatics and Its Applications (ISIA)*, Computer Science Department, University of M'sila, 2024, pp. 4–15. [Online]. Available: https://dspace.univ-msila.dz/handle/123456789/45404