Hardware-Level Side-Channel Attack Mitigation for PUF-Based Authentication in Smart Cities

Wafaa Mohammed Breesam
Department of Pharmacy, Babylon Technical Institute, Awsat Technical University, Babylon, Iraq
Wafaa.breesam@itu.edu.iq

Wafaa Mohammed Ridha
Department of Computer Networks and Software, Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, Babylon, Iraq
Wafaa.ridha@itu.edu.iq

Hayder Ali Hameed
General Directorate of Education Basrah, Basrah, Iraq
alhilifi@basrahaoe.iq

Mahmood A. Al-Shareeda
Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basrah, Iraq | College of Engineering, Al-Ayen University, Thi-Qar, Iraq
mahmood.alshareedah@stu.edu.iq (corresponding author)

Mohammed Amin Almaiah
Department of Computer Science, King Abdullah II IT School, The University of Jordan, Amman, Jordan
m.almaiah@ju.edu.jo

Rami Shehab
Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
Rtshehab@kfu.edu.sa

Received: 19 May 2025 | Revised: 27 June 2025, 2 July 2025, 10 July 2025, and 13 July 2025 | Accepted: 16 July 2025

 DOI: https://doi.org/10.48084/etasr.12233

ABSTRACT

Smart city infrastructure requires robust authentication mechanisms, yet existing lightweight techniques lack sufficient resistance to Side-Channel Attacks (SCAs) and biometric noise. This work presents a new authentication protocol that integrates a dual-Physically Unclonable Function (PUF) architecture with biometric binding, fuzzy extractors, response masking, and challenge randomization to strengthen immunity against SCA. Formal security analysis under the Real-Or-Random (ROR) model guarantees session-key secrecy, whereas informal analysis demonstrates resilience against impersonation, replay attacks, and physical-layer information leakage. Simulation results indicate that the recovery rate of the SCA key drops significantly from 84.2% to 6.7%. The protocol provides mutual authentication with an overhead of 2.1 kbit and a latency of 150 ms when supporting 1,000 devices, making it suitable for resource-limited settings. This paper presents a lightweight, secure, and scalable authentication scheme tailored for smart city applications.

Keywords-Side-Channel Attack (SCA); authentication protocol; smart cities; Physically Unclonable Function (PUF); lightweight cryptography; secure key agreement; fuzzy extractor

I. INTRODUCTION

The technological future of smart cities—cohesive urban ecosystems leveraging Internet of Things (IoT) technologies—has revolutionized the delivery of services across various industries, including healthcare, transportation, energy, and public safety [1-4]. The fundamental challenge in this area is the need for authentication protocols that are secure, efficient, and privacy-preserving, which authenticate users and devices over unsecured and potentially adversarial communication channels [5-8].

However, due to the resource constraints of IoT devices, dynamic mobility of users, and the rise of more sophisticated adversarial threats, securing interactions in a smart city environment is difficult [9-11]. Traditional cryptographic approaches, like public-key infrastructures or blockchain-based solutions, tend to require significant computational or energy resources, which may not be practical for resource-constrained devices [12, 13]. Moreover, the majority of lightweight schemes do not cover essential attacks like identity traceability, replay attacks, and side-channel leakage at the physical layer [14-17].

Physically Unclonable Functions (PUFs)–hardware primitives that yield unique and device-specific responses based on intrinsic manufacturing variations–have recently been explored in the literature to address these challenges [18-20]. Nonetheless, both PUFs and biometrics are also inherently noisy, and thus, fuzzy extractors should be used to generate reproducible secret keys [21-23].

Existing PUF-based mutual authentication schemes, however, still cannot efficiently achieve secure hardware-level protection against Side-Channel Attacks (SCAs), in particular those supported by fuzzy extractors and biometric inputs. To address these challenges, we propose a lightweight, hardware-insensitive, and biometric-based authentication protocol suited for smart city deployments, which includes the following key features:

- A new dual-PUF architecture with split-secret validation for higher robustness against hardware attacks.
- Response masking and challenge randomization to thwart traceability in SCA situations.
- Biometrics plus fuzzy extractors: A secure template syntax for stable noise tolerance.
- A formal proof for session key secrecy in the Real-Or-Random (ROR) model.

II. RELATED WORK

This section summarizes representative studies and notes important differences from the proposed approach. Several fuzzily secure cryptographic protocols have leveraged fuzzy extractors to assist comparative biometric or PUF noisy inputs for securely and repeatably generating keys instantiated from biometrics [24-28]. Although effective, the majority of these approaches still consider biometrics and PUFs as separate components rather than a single, interdependent source of entropy [29-30]. Additionally, most integrations of fuzzy extractors are only implemented at the logical authentication layers of the system, failing to address underlying hardware vulnerabilities [31-34].

PUFs have become popular as a security scheme for device-level authentication because they are naturally unique, unclonable, and require few resources. Initial endeavors concentrated on embedding static Challenge-Response Pairs (CRPs) with lightweight encryption schemes. For example, authors in [35] introduced a hash-based PUF protocol specifically for IoT devices that provides an efficient key exchange, but with poor resistance against physical attacks like Differential Power Analysis (DPA) and Electromagnetic Analysis (EMA). Similarly, authors in [36] introduced a drone-network authentication framework based on a single lightweight PUF instance. Although they proposed an energy-efficient scheme, it does not guarantee anonymity nor mitigate physical-layer leakage.

Authors in [37] implemented a new type of authentication method, which uses fuzzy extractors with PUF and biometric features for greater privacy preservation. This model provides mutual authentication, and it achieves anonymity without relying on hardware-level countermeasures against SCAs. Additionally, a physical probing scenario implies a single point of failure, as the system can be compromised if a single PUF instance is attacked.

III. PRELIMINARIES

A. System and Threat Model

In this section, we describe the system architecture and the attacker model that we assume for the proposed anonymous authentication protocol. The model is intended for realistic smart cities where devices and users communicate over open channels with logical and physical threats.

1. System model: The system is built around four key entities:
   - User (U_i): An individual who accesses services via a mobile device.
   - Mobile device (MD_i): Hosts biometric and dual-PUF modules for authentication and key derivation.
   - Gateway node (GW_j): Registers and validates identities, manages sensor interactions.
   - Sensor node (SN_i): Edge device that communicates within the smart city infrastructure.
2. Threat model: The threat model assumes adversaries capable of eavesdropping and replay attacks, Man-in-the-Middle (MitM) attacks, offline guessing attacks—where the attacker might use stolen or leaked information to guess user passwords or biometric templates—device compromise, SCAs, sensor cloning, and spoofing.

B. Mathematical Preliminaries

The improved approach relies on the three central building blocks: PUF, fuzzy extractor, and side-channel masking. Their

mathematical formulations are presented below to establish the foundation for the proposed scheme:

- Masked PUF: Suppose we denote the PUF function as P, and the challenge input as C, such that the output response is $R = P(C)$.
- Randomized challenges-pairs: To avoid correlating traces across sessions, each challenge C is transformed into a randomized challenge $C^* = Rand(C, \eta, T)$ based on a session nonce η and timestamp T: $C^* = C \oplus h(\eta \parallel T)$.
- Dual-PUF validation: Two physically independent PUF instances, P_1 and P_2, are deployed for masked response generation and auxiliary split-secret validation, respectively.

C. Side-Channel Attacks

SCAs recover sensitive information from physical emanations such as power traces, Electromagnetic (EM) radiation, or execution time. Typical SCA types include Simple Power Analysis (SPA), DPA, and EMAs. The defense techniques combine:

- Response masking: Introduces distortion to the PUF responses.
- Challenge Randomization: Ensures that static CRPs are not reused.
- Dual-PUF architecture: Spreads entropy over two hardware modules to enhance robustness.

IV. PROPOSED SCHEME

In this section we introduce the mathematical preliminaries and the main components of the proposed improved authentication protocol, as shown in Figure 1. In the smart city topology, the scheme provides new countermeasures against hardware-level SCAs using a combination of response masking, randomized CRPs, and dual-PUF architectures, enhancing the resistance of the authentication environment. The proposed protocol incorporates user biometrics as a secondary entropy source to enhance the binding of identity and her/his secret from key sharing [38-40]. This paper focuses on the implementation based on fingerprint images as a biometric modality because of their pervasive use in mobile smart devices. A fuzzy extraction protocol using Bose–Chaudhuri–Hocquenghem (BCH) error-correcting code is used to stabilize biometric inputs and to generate reproducible cryptographic keys. Table I shows the notation used in this paper.

A. System Setup Phase

This phase bootstraps the global parameters and configures sensor nodes. For each sensor, the gateway creates two challenge inputs for a dual-PUF block and computes masked responses with random masks to resist SCAs. These credentials are retained locally and used for subsequent authentication. The gateway node GW_j initializes the elliptic curve group parameters and selects its private master key $GW \in Z_q$. For each sensor node SN_i, it assigns a unique identity SID_i and generates challenges C_{1i} and C_{2i} for PUF instances P_1 and P_2, respectively. Masked responses are computed as:

$$R'_{2i} = P_2(C_{2i}) \oplus M_2 \quad (1)$$

The gateway securely stores $\{SID_i, C_{1i}, C_{2i}, R'_{1i}, R'_{2i}\}$ and publishes the generator functions $Gen(\cdot)$, $Rep(\cdot)$, and the PUF parameters.

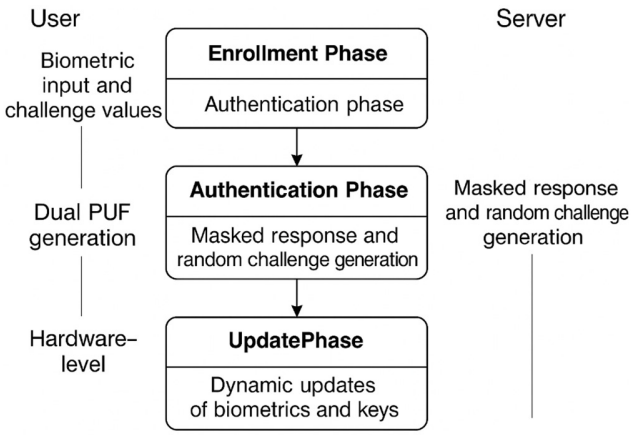

Fig. 1. Workflow diagram depicting the phases of the proposed protocol.

TABLE I. SUMMARY OF NOTATIONS USED

Symbol	Description
UID_i	Identity of user i
SID_i	Identity of sensor node i
$P(C)$	Output of PUF function for challenge C
P_1, P_2	Two independent PUF instances
C, C^*	Challenge and randomized challenge input
R, R'	Raw and masked PUF response
M	Random mask generated using Pseudorandom Number Generator (PRNG)
B_i	Biometric data of user i
α_i, β_i	Outputs from fuzzy extractor (Gen)
θ, ζ	Reconstructed secrets using fuzzy extractor (Rep)
SK	Session key
R_3, R_4, R_5	Nonces generated during authentication
T_1, T_2, T_3	Timestamps used in session freshness
$h(\cdot)$	Collision-resistant hash function
$\oplus$	Bitwise XOR operation
Adv_A^{ROR}	Adversary advantage in ROR model

B. Sensor Node Registration Phase

In this step, each sensor node sends out its identity and response to the gateway and initiates the registration process. The gateway authenticates and computes helper data based on fuzzy extractors applied to the protected PUF responses. It yields authentication tokens that can be used to authenticate the sensor. Sensor node SN_i initiates registration by transmitting the message: $Req_1 = \{SID_i^*, R_1\}$. Upon verification of SID_i^*, the gateway derives $(\theta_i, \beta_i) = Gen(R'_{1i})$, $(\zeta_i, \beta'_i) = Gen(R'_{2i})$. Authentication tokens are generated as:

$$\begin{aligned} A_1 &= h(SID_i \parallel GW), \\ A_2 &= A_1 \oplus h(SID_i \parallel R_1), \\ A_3 &= \beta_i \oplus h(A_1 \parallel R_1 \parallel SID_i) \end{aligned} \quad (2)$$

The gateway responds with: $Res_1 = \{A_2, A_3\}$. The sensor stores $\{A_2, A_3\}$ and the challenge pairs for future use.

C. User Registration Phase

This stage enables the user to securely register with the system. The user's biometric input is processed through fuzzy extractors to produce template keys. The user U_i selects a password PW_i and identity UID_i, and inputs biometric data B_i into the mobile device MD_i. Using fuzzy extractors $(\alpha_i, \beta_i) = Gen(P_1(B_i))$, $(\alpha_i, \beta_i) = Gen(P_2(B_i))$ the device computes:

$$\beta_i^* = \beta_i \oplus h(UID_i \parallel PW_i \parallel P_1(B_i)),$$
$$\beta_i^* = \beta_i' \oplus h(UID_i \parallel PW_i \parallel P_2(B_i)), \quad (3)$$
$$SID_i^* = SID_i \oplus h(UID_i \parallel \alpha_i \parallel R_2)$$

The parameters $\{\beta_i^*, SID_i^*\}$ are stored locally in the secure memory of MD_i.

D. Authentication and Key Negotiation Phase

This is the main protocol for authentication. It is a challenge-response-based communication, where both sides negotiate CRPs, nonces, and hash-based tokens between the user, the service operator, and the gateway. This phase relies on the dual PUFs, fuzzy extractor reconstruction, and time-dependent masking to achieve mutual authentication and retrieves a shared session key that is secure against side-channel leakage. The authentication phase begins with U_i inputting UID_i, PW_i, and biometric B_i. The device reconstructs secrets via:

$$a_i = Rep\left(P_1(B_i), \beta_i^* \oplus h\big(UID_i \parallel PW_i \parallel P_1(B_i)\big)\right),$$
$$\zeta_i = Rep\left(P_2(B_i), \beta_i^* \oplus h\big(UID_i \parallel PW_i \parallel P_2(B_i)\big)\right) \quad (4)$$

A session nonce R_3 is generated, and the following values are computed:

$$B_3 = (R_3 \parallel SID_i) \oplus h(B_1 \parallel B_2 \parallel T_1),$$
$$B_4 = h(B_1 \parallel R_3 \parallel B_2 \parallel T_1), \quad (5)$$
$$Auth_1 = \{B_1, B_3, B_4, T_1\}$$

After validation at GW_j, a second nonce R_4 is generated and sent as part of:

$$C_1 = (R_3 \parallel R_4) \oplus h(SID_i \parallel \theta_i \parallel A_1 \parallel T_2),$$
$$C_2 = h(SID_i \parallel R_4 \parallel A_1 \parallel \theta_i \parallel T_2), \quad (6)$$
$$Auth_2 = \{\delta_i, C_1, C_2, T_2\}$$

At SN_i, after response validation, a third nonce R_5 is generated. The session key is computed as:

$$SK_{SU} = h(R_3 \parallel R_5 \parallel \theta_i \parallel \zeta_i) \quad (7)$$

The additional message fields are:

$$C_3 = R_5 \oplus h(\theta_i \parallel R_4 \parallel T_3),$$
$$C_4 = h(SID_i \parallel R_4 \parallel R_5 \parallel \theta_i \parallel T_3),$$
$$D_1 = h(R_3 \parallel R_4 \parallel \theta_i \parallel SID_i \parallel SK_{SU}), \quad (8)$$
$$Auth_3 = \{C_3, C_4, D_1, T_3\}$$

Upon reception, GW_j and then MD_i validate the hash chains and derive:

$$SK_{US} = h(R_3 \parallel R_5 \parallel \theta_i \parallel \zeta_i) \quad (9)$$

If and only if all verifications succeed, mutual authentication is established and $SK_{US} = SK_{SU}$.

E. Parameter Update Phase

This stage permits the users to locally change their password or biometric template without the intervention of the gateway. The user U_i can update PW_i and B_i locally. After verifying the current parameters, the mobile device prompts for new inputs and recalculates:

$$(\alpha_{inew}, \beta_{inew}) = Gen\big(P_1(B_{inew})\big),$$
$$(\zeta_{inew}, \beta_{i'new}) = Gen\big(P_2(B_{inew})\big) \quad (10)$$

The updated tokens are:

$$\beta_{inew}^* = \beta_{inew} \oplus h\big(UID_i \parallel PW_{inew} \parallel P_1(B_{inew})\big),$$
$$\beta_{i'new}^* = \beta_{i'new} \oplus h\big(UID_i \parallel PW_{inew} \parallel P_2(B_{inew})\big) \quad (11)$$

The old tokens are replaced with the new values in the secure memory of MD_i without requiring gateway interaction.

F. Hardware-level Side-Channel Attack Mitigation

To strengthen the resilience of the proposed authentication scheme, response masking, randomized challenge-response pairing, and dual-PUF architecture are introduced as three robust and lightweight countermeasures:

- Techniques for masking responses: Even though PUFs are unclonable, they emit information that can be exploited with DPA due to their stable response patterns. The major benefit of masking is the added statistical noise that corrupts the physical signal of the PUF response.
- Randomized challenge-response pairing: Another type of vulnerability in PUF-based systems is the repeated usage of static CRPs, which can be profiled and compromised through correlation attacks. To remedy this, the proposed scheme employs session-specific randomization of CRP selection. The XOR of a nonce and a hash derived from the timestamp dynamically modifies each challenge. This duality means that even if the same logical puzzle is reused from session to session, its physical representation varies each time.
- Dual-PUF architecture with split secret validation: To strengthen the authentication scheme against sophisticated physical attacks or contextual fault injection, a dual-PUF model is combined.
- Security implications: These hardware-level countermeasures together harden the system against physical attackers. Through masking and randomized CRPs, we ensure variability of traces and thus avoid deterministic leakages, whereas fault tolerance against local compromise is achieved through the dual-PUF architecture.

V. SECURITY ANALYSIS

A. *Formal Security Analysis*

We adopt the ROR oracle-based model to analyze the session key secrecy of the proposed protocol, as shown in Figure 2. This model evaluates whether an adversary can distinguish a real session key from a randomly generated one with non-negligible advantage.

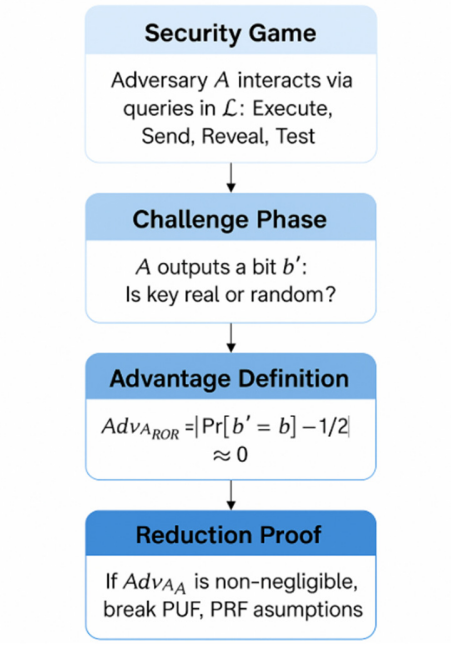

Fig. 2. ROR model steps.

Let A be a Probabilistic Polynomial-Time (PPT) adversary that interacts with the system through the following queries:

- $Execute(U_i, SN_i)$: Returns a full transcript of a passive run between user U_i and sensor node SN_i.
- $Send(P, m)$: Sends a message m to protocol participant P and returns the response.
- $Reveal(P)$: Reveals the session key of party P if a session has been established.
- $Test(P)$: Returns either the real session key or a random string of the same length, depending on a hidden bit $b \in \{0,1\}$.

The adversary's goal is to distinguish the real key from a random one. The adversary's advantage is defined as the following equation:

$$Adv_{\mathcal{A}}^{ROR} = \left| Pr[\mathcal{A}_{wins}] - \frac{1}{2} \right| \quad (12)$$

Theorem 1: Under the assumptions that the hash function $h(\cdot)$ is collision-resistant and that PUF responses are unpredictable and masked, the advantage $Adv_{\mathcal{A}}^{ROR}$ is negligible in the random oracle model.

Proof sketch: The session key is derived as: $SK = h(\vartheta \parallel \zeta \parallel R_3 \parallel R_5)$, where $\theta = Rep(P_1(C_1), \beta_1)$ and $\zeta = Rep(P_2(C_2), \beta_2)$:

- An adversary cannot guess or reconstruct SK without knowing both PUF outputs θ and ζ, as well as the nonces R_3 and R_5, all of which are session-specific and hidden.
- The masked response $R' = P(C) \oplus M$, where $M = h(\eta \parallel T)$, introduces non-determinism, rendering power and timing observations ineffective for direct inference.
- Even with access to multiple transcripts via $Execute$ and $Send$, and exposure to partial keys via $Reveal$, the adversary cannot correlate internal secrets due to the uniqueness and non-reusability of PUF responses.
- The $Test$ oracle only returns real or random keys after session establishment, and any adversary's ability to correctly guess the hidden bit b approaches random guessing, as the following equation:

$$Adv_{\mathcal{A}}^{ROR} \leq \varepsilon(negligible) \quad (13)$$

Hence, the proposed scheme ensures session key indistinguishability under the ROR model.

B. *Informal Security Analysis*

This section provides an informal analysis of the security properties of the proposed authentication scheme against a wide variety of attack vectors and adversarial goals.

- Mutual authentication: A three-way chain of cryptographic challenges and session-specific nonces is exchanged among the user U, the gateway GW, and the sensor node SN_i to ensure mutual authentication. Each one computes a unique hash (B_4, C_2, D_1) that binds the session's associated values, identities, and nonces. This prevents unauthorized devices or users from participating in the protocol.
- Anonymity of users & untraceability: To protect user privacy, the real identity SID_i is not transferred in plaintext form. Instead, it is hidden using a dynamic hash mask: $SID_i^* = SID_i \oplus h(UID_i \| \alpha_i \| R_2)$ and the biometric-derived value α_i changes with each session. Thus, SID_i^* appears unique per session.
- Resistance to replay attacks: Timestamps (T_i) and random nonces (R_3, R_4, R_5) are included in all the major authentication messages. Replay attacks are prevented as the gateway and sensor nodes rejects messages with an invalid timestamp or a reused timestamp.
- Resistance to impersonation attacks: An adversary cannot generate valid authentication messages without the user's secrets (biometric template, password, or PUF output). Freshness tokens and biometric dependencies ensure intercepted messages cannot be reused or modified.
- Session key secrecy: The session key is built as: $SK = h(\theta || \zeta || R_3 || R_5)$, where θ and ζ are produced from two different PUF instances, and R_3 and R_5 are fresh nonces from the user and sensor, respectively. These components are session-specific, unforeseeable, and yield a session key

that is indistinguishable from random, even if other session parameters are only partially compromised.

- Resilience against SCAs: Session-randomized values mask PUF outputs as: $R' = P(C) \oplus M$, $M = h(\Delta T)$. This masking adds uncertainty to the physical power consumption and EM emissions, undermining SCAs such as DPA or EMA.
- Forward and backward secrecy: Forward secrecy ensures past session keys remain secure even if a current key is compromised, whereas backward secrecy protects future keys from compromise of earlier sessions.

C. Security Comparison

We evaluate the robustness of the proposed scheme by comparing it against two recent PUF-based authentication protocols presented in [35] and [36], as well as the original model in [37] on which this work builds. This comparison focuses on core security features, including mutual authentication, session key secrecy, anonymity, resistance to replay attacks, and resistance to SCAs. The results are summarized in Table II using a symbolic checklist: ✓ indicates support for the feature, ✗ indicates lack of support.

TABLE II. SECURITY FEATURE COMPARISON OF PUF-BASED AUTHENTICATION SCHEMES

Security feature	Proposed scheme	[37]	[36]	[35]
PUF integration	✓	✓	✓	✓
Mutual authentication	✓	✓	✓	✓
User anonymity	✓	✓	✗	✓
Resistance to replay attack	✓	✓	✓	✓
Impersonation protection	✓	✓	✗	✗
SCA resistance	✓	✗	✗	✗
Forward & backward secrecy	✓	✓	✗	✓
Fuzzy extractor usage	✓	✓	✗	✗
Session key secrecy	✓	✓	✗	✓
Formal security model (ROR)	✓	✗	✗	✗

This comparative analysis highlights the significant security improvements offered by the proposed approach over existing state-of-the-art methods.

VI. PERFORMANCE AND SIDE-CHANNEL RESISTANCE EVALUATION

This section discusses the efficiency of the proposed authentication scheme in terms of computational complexity, communication overhead, and resistance to side-channel leakage. To verify performance, the protocol was executed on a Raspberry Pi Pico (ARM Cortex-M0+). The full authentication cycle completed in 132 ms per session, with a memory footprint of 32 KB (flash) / 9.4 KB (RAM). Compared to the scheme in [37], the construction incurs minimal overhead in exchange for improved side-channel security. The energy consumption per session was approximately 0.18 mJ, demonstrating the protocol's potential in practical smart city IoT scenes.

To assess scalability, the latency was measured as the number of concurrently authenticating devices increased. As shown in Figure 3, the latency scales somewhat with the number of devices (from 25 ms at 100 devices to approximately 150 ms at 1,000 devices).

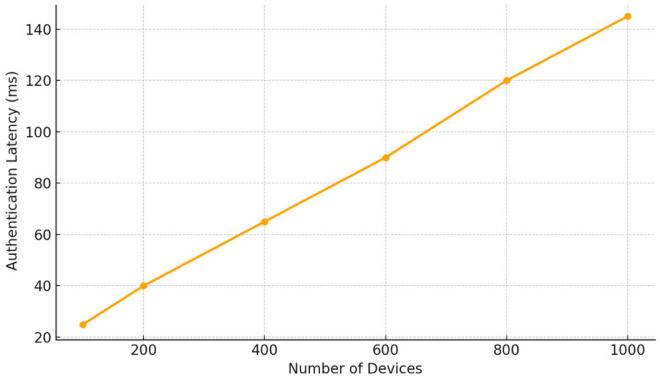

Fig. 3. Authentication latency versus device count.

A. Execution Efficiency and Lightweight Overhead

The integration of dual-PUF units and response masking introduces only two additional hash operations beyond the baseline protocol in [37], preserving a lightweight profile. Figure 4 presents a comparison of the hash-based computation cost.

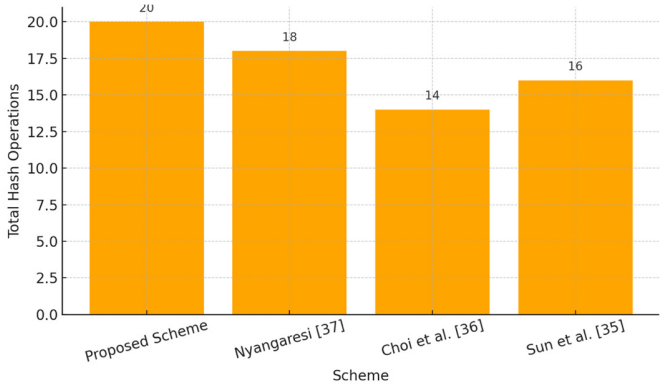

Fig. 4. Comparison of computation cost in hash operations.

B. Communication Overhead and Scalability

Efficient bandwidth usage is a necessity for smart city deployments. The total size of the messages exchanged during the 4-step authentication process is around 2.1 kbit, comprising hashed identifiers, masked CRPs, and timestamps. Figure 5 illustrates the comparative communication cost across schemes.

C. Energy Consumption

The proposed protocol requires approximately 0.18 mJ per authentication session on a Raspberry Pi Pico (Cortex-M0+). As shown in Figure 6, this energy usage is marginally higher than in [36] and [37] due to the extra cryptographic overhead from dual-PUF evaluations and fuzzy extractor operations.

Nevertheless, the energy cost remains acceptable for low-power IoT devices used in smart city infrastructure.

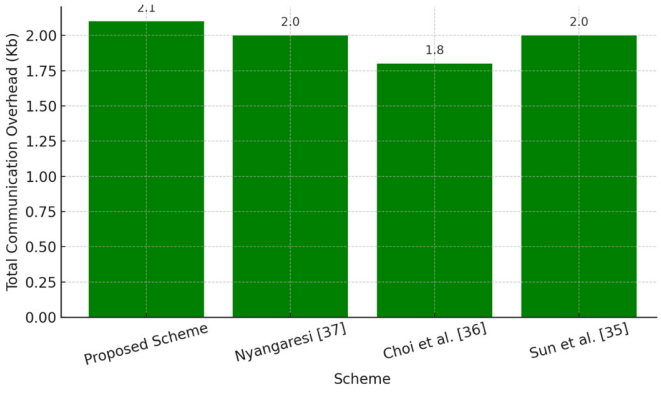

Fig. 5. Comparison of communication overhead.

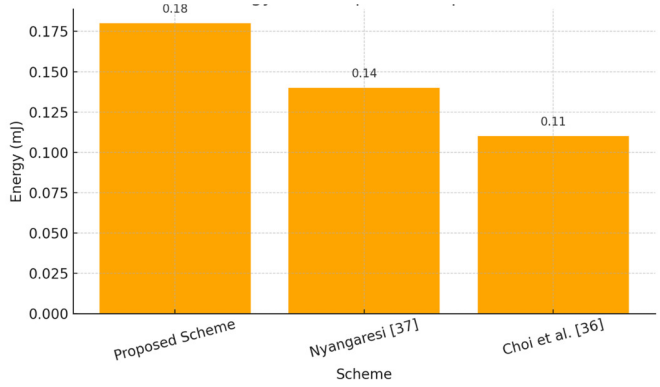

Fig. 6. Comparison of energy consumption.

D. Side-Channel Attack Simulation Results

The efficiency of masking and challenge randomness was evaluated using simulations on the ChipWhisperer-Lite platform. In the absence of a physical prototype, simulations were conducted to preliminarily assess resistance to SCAs. The simulation environment was configured using the ChipWhisperer-Lite platform along with a simulated PUF module written in Python, capable of emulating both masked and unmasked responses. The experiment setup was as follows:

- Target function: XOR-masked PUF response using session-dependent masks.
- Attack type: DPA using 1,000 simulated traces.
- Baseline: Single-PUF system without masking.

1) Success Rate of Side-Channel Attacks

Key recovery success dropped sharply in a simulated side-channel trace analysis using 1,000 traces on the ChipWhisperer-Lite platform. As shown in Figure 7, the proposed masked dual-PUF architecture reduced the success rate to less than 6.7%, whereas the unmasked single-PUF setup exhibited a success rate of 84.2%, indicating considerable physical-layer resilience against DPA attacks. This confirms the effectiveness of masking and entropy splitting under practical attack conditions. The proposed masking and randomized challenge mechanisms significantly distorted observable patterns, reducing trace correlation from 0.91 (baseline) to less than 0.12 after masking.

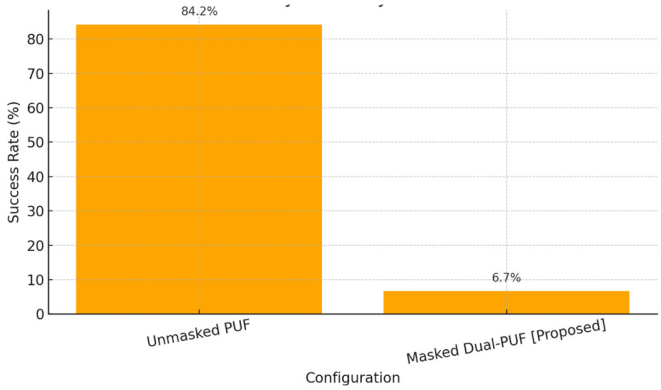

Fig. 7. Success rate of key recovery under SCA simulation.

E. Summary of Performance-Security Trade-off

To confirm the practicality of the proposed scheme, we summarize its key performance and security aspects. This trade-off demonstrates that the improved physical-layer protections, namely response masking and dual-PUF entropy splitting, introduce minimal overhead, rendering the protocol both secure and efficient for smart city scenarios:

- Security: Resistance to SCAs, impersonation, and replay attacks is supported by this protocol.
- Computational overhead: Only two hash operations more than typical lightweight constructions.
- Communication cost: Extra cost of 200–300 bits required for dual-PUF and masking operations.
- Hardware footprint: Remains low, suitable for devices with limited memory (e.g. Cortex-M0+).

VII. CONCLUSION AND FUTURE WORK

In this paper, a lightweight secure authentication protocol exploiting biometric binding, dual-Physically Unclonable Function (PUF) architecture, response masking, and challenge randomization is proposed for smart cities. A formal security proof under the Real-Or-Random (ROR) model demonstrates session key indistinguishability and strong simulation-based resilience to Side-Channel Attacks (SCAs), reducing the probability of key recovery from 84.2% to less than 6.7%. The protocol provides mutual authentication with only 2.1 kbit overhead and less than 150 ms latency for 1,000 devices, demonstrating scalability and cost-effectiveness for Internet of Things (IoT) systems.

The key contributions of this work include:

- Dual-PUF with palindromic-secret inversion: Rather than using a single PUF (e.g., [36], [37]), the dual-PUF design uses a secret that is appropriately split. This spreads the entropy and thus avoids a single-point adversary, offering

more resilience against probing operations at the hardware level.

- Response masking using time-variant session nonces: The proposed masking mechanism adds trace-level noise to mitigate side-channel leakage and outperforms previous static PUF-based schemes.
- Biometric-PUF integration via fuzzy extractors: The scheme integrates a fuzzy extractor at hardware and biometric layers to enable stable key derivation despite input noise, while preserving anonymity and template protection.
- High security gains with minimal cryptographic overhead: Only two additional hash operations are added per session, resulting in a 0.18 mJ of energy consumption per section. This retains the scheme's suitability for constrained IoT platforms, such as the Cortex-M0+.
- Formal and informal security validation: Unlike prior work lacking formal analysis, this protocol was validated symbolically (ROR model), and empirically (simulated Differential Power Analysis (DPA) attacks) in multiple areas.

These contributions demonstrate that the proposed protocol is a major leap forward compared to existing solutions, especially for its resistance against SCAs, physical layer robustness, and scalability in dense IoT deployments. Further work includes deploying the protocol on actual hardware (e.g., STM32, Raspberry Pi Pico with PUF modules) and performing empirical DPA/Electromagnetic Analysis (EMA) attacks. Future directions include incorporating adaptive biometric-PUF fusion. Other expected developments include group authentication, dynamic access control, and post-quantum security. Formal verification using tools such as ProVerif will also contribute to robustness against sophisticated threats.

ACKNOWLEDGEMENT

This research is part of a collaborative, government-supported initiative to promote interdisciplinary research among academic institutions across Iraq, Jordan, and Saudi Arabia. Each author brought domain-specific expertise, enabling a robust and well-rounded solution applicable to smart city security.

FUNDING

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. kfu251449).

REFERENCES

[1] S. Pandya *et al.*, "Federated learning for smart cities: A comprehensive survey," *Sustainable Energy Technologies and Assessments*, vol. 55, Feb. 2023, Art. no. 102987, https://doi.org/10.1016/j.seta.2022.102987.

[2] A. Khang, S. K. Gupta, S. Rani, and D. A. Karras, *Smart Cities: IoT Technologies, Big Data Solutions, Cloud Platforms, and Cybersecurity Techniques*, 1st ed. Boca Raton, FL, USA: CRC Press, 2023, https://doi.org/10.1201/9781003376064.

[3] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Towards Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Access*, vol. 9, pp. 113226–113238, 2021, https://doi.org/10.1109/ACCESS.2021.3104148.

[4] M. A. Al-Shareeda *et al.*, "Provably Secure with Efficient Data Sharing Scheme for Fifth-Generation (5G)-Enabled Vehicular Networks without Road-Side Unit (RSU)," *Sustainability*, vol. 14, no. 16, pp. 1–19, Aug. 2022.

[5] F. A. Almalki *et al.*, "Green IoT for Eco-Friendly and Sustainable Smart Cities: Future Directions and Opportunities," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 178–202, Feb. 2023, https://doi.org/10.1007/s11036-021-01790-w.

[6] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, "PUF-Based Authentication and Key Agreement Protocols for IoT, WSNs, and Smart Grids: A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8205–8228, June 2022, https://doi.org/10.1109/JIOT.2022.3142084.

[7] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Password-Guessing Attack-Aware Authentication Scheme Based on Chinese Remainder Theorem for 5G-Enabled Vehicular Networks," *Applied Sciences*, vol. 12, no. 3, Feb. 2022, Art. no. 1383, https://doi.org/10.3390/app12031383.

[8] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-Fog: A Novel Anonymous Authentication Scheme for 5G-Enabled Vehicular Fog Computing," *Mathematics*, vol. 11, no. 6, Mar. 2023, Art. no. 1446, https://doi.org/10.3390/math11061446.

[9] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustainable Cities and Society*, vol. 66, Mar. 2021, Art. no. 102655, https://doi.org/10.1016/j.scs.2020.102655.

[10] N. M. Alzahrani and F. A. Alfouzan, "Augmented Reality (AR) and Cyber-Security for Smart Cities—A Systematic Literature Review," *Sensors*, vol. 22, no. 7, Apr. 2022, Art. no. 2792, https://doi.org/10.3390/s22072792.

[11] B. N. Bukke, K. Manjunathachari, and S. Sabbavarapu, "Implementation of a Finite Impulse Response Filter using PUFs to Avoid Trojans," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12151–12157, Dec. 2023, https://doi.org/10.48084/etasr.6133.

[12] M. H. Panahi Rizi and S. A. Hosseini Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," *Internet of Things*, vol. 20, Nov. 2022, Art. no. 100584, https://doi.org/10.1016/j.iot.2022.100584.

[13] A. K. M. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," *Expert Systems*, vol. 39, no. 5, June 2022, Art. no. e12753, https://doi.org/10.1111/exsy.12753.

[14] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework," *Information Systems Frontiers*, vol. 24, no. 2, pp. 393–414, Apr. 2022, https://doi.org/10.1007/s10796-020-10044-1.

[15] S. Sharma and N. Mishra, "Horizoning recent trends in the security of smart cities: Exploratory analysis using latent semantic analysis," *Journal of Intelligent & Fuzzy Systems*, vol. 46, no. 1, pp. 579–596, Jan. 2024, https://doi.org/10.3233/JIFS-235210.

[16] S. Otoom, "Risk auditing for Digital Twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22–35, Jan. 2025, https://doi.org/10.63180/jcsra.thestap.2025.1.3.

[17] A. AlShuaibi, M. W. Arshad, and M. Maayah, "A Hybrid Genetic Algorithm and Hidden Markov Model-Based Hashing Technique for Robust Data Security," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 42–56, May 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.6.

[18] A. Al-Meer and S. Al-Kuwari, "Physical Unclonable Functions (PUF) for IoT Devices," *ACM Computing Surveys*, vol. 55, no. 14s, July 2023, Art. no. 314, https://doi.org/10.1145/3591464.

[19] A. Yadav, S. Kumar, and J. Singh, "A Review of Physical Unclonable Functions (PUFs) and Its Applications in IoT Environment," in *Ambient*

Communications and Computer Systems: Proceedings of RACCCS 2021, Ajmer, India, 2022, pp. 1–13, https://doi.org/10.1007/978-981-16-7952-0_1.

[20] D. P. Podugu, A. K. Kumari, and S. Sabbavarapu, "Intellectual Property Design with PUF-based Hardware Security," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15559–15563, Aug. 2024, https://doi.org/10.48084/etasr.7413.

[21] A. Davarasan, J. Samual, K. Palansundram, and A. Ali, "A Comprehensive Review of Machine Learning Approaches for Android Malware Detection," *Journal of Cyber Security and Risk Auditing*, vol. 2024, no. 1, pp. 38–60, Dec. 2024, https://doi.org/10.63180/jcsra.thestap.2024.1.5.

[22] R. Djehaiche, S. Aidel, A. Sawalmeh, N. Saeed, and A. H. Alenezi, "Adaptive Control of IoT/M2M Devices in Smart Buildings Using Heterogeneous Wireless Networks," *IEEE Sensors Journal*, vol. 23, no. 7, pp. 7836–7849, Apr. 2023, https://doi.org/10.1109/JSEN.2023.3247007.

[23] A. Aldossary, T. Algirim, I. Almubarak, and K. Almuhish, "Cyber Security in Data Breaches," *Journal of Cyber Security and Risk Auditing*, vol. 2024, no. 1, pp. 14–22, Dec. 2024, https://doi.org/10.63180/jcsra.thestap.2024.1.3.

[24] S. Biswas, R. S. Goswami, and K. H. K. Reddy, "Advancing quantum steganography: a secure IoT communication with reversible decoding and customized encryption technique for smart cities," *Cluster Computing*, vol. 27, no. 7, pp. 9395–9414, Oct. 2024, https://doi.org/10.1007/s10586-024-04429-z.

[25] N. Minhas, "Post-Quantum Authentication Scheme for IoT Security in Smart Cities." Preprints, July 30, 2024, https://doi.org/10.20944/preprints202407.2309.v1.

[26] S. Ang, M. Ho, S. Huy, and M. Janarthanan, "Utilizing IDS and IPS to Improve Cybersecurity Monitoring Process," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 77–88, July 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.10.

[27] M. A. Almedires, A. Elkhalil, and M. Amin, "Adversarial Attack Detection in Industrial Control Systems Using LSTM-Based Intrusion Detection and Black-Box Defense Strategies," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 4–22, May 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.2.

[28] B. Almelehy, M. Ahmad, G. Nassreddine, M. Maayah, and A. Achanta, "Analytical Analysis of Cyber Threats and Defense Mechanisms for Web Application Security," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 57–76, July 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.4.

[29] S. Singh, A. Pise, O. Alfarraj, A. Tolba, and B. Yoon, "A cryptographic approach to prevent network incursion for enhancement of QoS in sustainable smart city using MANET," *Sustainable Cities and Society*, vol. 79, Apr. 2022, Art. no. 103483, https://doi.org/10.1016/j.scs.2021.103483.

[30] S. A. M. Taqi and S. Jalili, "LSPA-SGs: A lightweight and secure protocol for authentication and key agreement based Elliptic Curve Cryptography in smart grids," *Energy Reports*, vol. 8, no. 9, pp. 153–164, Nov. 2022, https://doi.org/10.1016/j.egyr.2022.06.096.

[31] S. Gupta *et al.*, "Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications," *Sustainability*, vol. 15, no. 6, Mar. 2023, Art. no. 5346, https://doi.org/10.3390/su15065346.

[32] A. Aldosary and M. Tanveer, "PAAF-SHS: PUF and authenticated encryption based authentication framework for the IoT-enabled smart healthcare system," *Internet of Things*, vol. 26, July 2024, Art. no. 101159, https://doi.org/10.1016/j.iot.2024.101159.

[33] N. Frederick and A. Ali, "Enhancing DDoS Attack Detection and Mitigation in SDN Using Advanced Machine Learning Techniques," *Journal of Cyber Security and Risk Auditing*, vol. 2024, no. 1, pp. 23–37, Dec. 2024, https://doi.org/10.63180/jcsra.thestap.2024.1.4.

[34] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021, https://doi.org/10.1109/ACCESS.2021.3073203.

[35] D.-Z. Sun, Y.-N. Gao, and Y. Tian, "On the Security of a PUF-Based Authentication and Key Exchange Protocol for IoT Devices," *Sensors*, vol. 23, no. 14, July 2023, Art. no. 6559, https://doi.org/10.3390/s23146559.

[36] J. Choi, S. Son, D. Kwon, and Y. Park, "A PUF-Based Secure Authentication and Key Agreement Scheme for the Internet of Drones," *Sensors*, vol. 25, no. 3, Feb. 2025, Art. no. 982, https://doi.org/10.3390/s25030982.

[37] V. O. Nyangaresi, A. A. AlRababah, G. K. Yenurkar, R. Chinthaginjala, and M. Yasir, "Anonymous Authentication Scheme Based on Physically Unclonable Function and Biometrics for Smart Cities," *Engineering Reports*, vol. 7, no. 1, Jan. 2025, Art. no. e13079, https://doi.org/10.1002/eng2.13079.

[38] Z. S. Alzaidi, A. A. Yassin, Z. A. Abduljabbar, and V. O. Nyangaresi, "A Fog Computing and Blockchain-based Anonymous Authentication Scheme to Enhance Security in VANET Environments," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19143–19153, Feb. 2025, https://doi.org/10.48084/etasr.8663.

[39] N. Ammour, Y. Bazi, and N. Alajlan, "Multimodal Approach for Enhancing Biometric Authentication," *Journal of Imaging*, vol. 9, no. 9, Sept. 2023, Art. no. 168, https://doi.org/10.3390/jimaging9090168.

[40] A. Tareef, K. Al-Tarawneh, and A. Sleit, "Block-based Watermarking for Robust Authentication and Integration of GIS Data," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16340–16345, Oct. 2024, https://doi.org/10.48084/etasr.8197.