

APELS: An Adaptive PUF-ECC Lightweight Security Framework for Encryption and Authentication in Resource-Constrained IoT Networks

(A Survey and Novel Framework for Securing the Internet of Things)

Gaddapaara Swetha , Dr. J. Pradeep Kumar
Malla Reddy University

Abstract: Healthcare, agriculture, industry and smart cities are all showing growth in numbers of IoT devices that require lightweight security mechanisms which are bound by strict resource constraints. The traditional security protocols like RSA and TLS are inefficient in terms of computation and energy usage, and symmetric-key techniques do not have a forward secrecy problem or are hard to scale. APELS is an Adaptive PUF-ECC Lightweight Security framework which combines Elliptic Curve Diffie-Hellman (ECDH) key agreement and Physical Unclonable Function (PUF) device authentication in edge-fog-cloud architecture is presented in this paper. For implementing dynamic control of the session key rotation interval, an adaptive trust controller is proposed that calculates a composite trust score based on the authentication latency, energy consumption and PUF reliability. The framework uses elliptic-curve based shared secret generation and trust-driven key rotation model, increases security, and reduces overhead. The simulation results show that APELS is more energy efficient, faster in terms of latency, has less communication overhead, and provides enhanced security against replay, impersonation, man-in-the-middle, and key extraction attacks compared to blockchain authentication schemes such as ECC-only, RSA-2048, and PBFT.

Keywords: Internet of Things security; lightweight authentication; elliptic curve cryptography; physical unclonable function; edge-fog-cloud architecture; adaptive key management

1. INTRODUCTION

The Internet of Things now enables tens of billions of sensors, actuators and embedded controllers to be continuously exchanging data across industrial automation lines, precision agriculture fields, remote health monitors and smart city infrastructure. This level of interconnection has made IoT networks an appealing target for bad actors, who can use a single breached node to compromise an entire deployment and send data to an attacker, or to send false data to the other nodes and disrupt the physical processes. Most IoT endpoints have significantly limited resources for processing power, memory, energy budget, and communication bandwidth, making it impractical to apply traditional security protocols that were

originally designed for networked computers on the server and desktop class.

The key issues of this work are the lack of secure and feasible encryption and authentication solutions on constrained hardware that imposes an unfair burden on the security strength and usability of the hardware. The full public key infrastructures based on RSA or standard elliptic curve TLS handshakes are computation and energy intensive which reduces battery life, and add latency not suitable for real-time control loops. Such schemes are purely symmetric-key schemes, which minimize this overhead but require a pre-shared secret that is hard to provision, maintain, rotate and scale to other participants, and they do not offer forward secrecy in general. Hardware-based device fingerprinting (DFP) like physical unclonable functions (PUF) provides lightweight fingerprinting of a device, but does not typically include a formal key agreement protocol and relies on other protocols that reintroduce the overhead that PUFs aim to eliminate.

A survey of the recent literature (Section 2) reveals that the proposals focus on the optimization of a single axis (elliptic curve efficiency, blockchain based decentralization, or PUF based fingerprinting) rather than on latency, energy, communication overhead and multi-vector attack resilience in common experimental settings. Adaptive re-keying based on the observed network and trust conditions are under-studied as well, and few designs describe a full edge-fog-cloud pathway, including revocation of devices from the fog to the cloud, audit logging, and the authentication handshake itself.

To conquer this, in this paper, we introduce an adaptive PUF-ECC lightweight security framework which integrates ephemeral elliptic curve Diffie-Hellman key agreement (ECDH-KA) with PUF based device fingerprinting (DFP) in a three-tier edge-fog-cloud architecture. A gateway resident adaptive trust controller calculates a combined authentication latency, energy usage, and PUF response reliability trust score,

with which it determines the rate of session key rekeying; when conditions are stable, it increases the sense of security, resulting in an increase in the frequency of rekeying, while when anomalies are observed, it strengthens the sense of insecurity, causing the rekeying frequency to decrease. It is designed in such a way that only lightweight elliptic curve and hash functions are performed on constrained edge nodes, while fog and cloud tiers have more computational power to allow for heavier bookkeeping, trust scoring and revocation management.

The key contributions of this paper are summarized below.

- ❖ APELS, an elliptic curve key agreement and PUF-based device fingerprinting to provide a hybrid encryption and authentication framework across an edge-fog-cloud architecture.
- ❖ A new formulation of adaptive trust-weighted key rotation, based on the observed latency, energy and PUF reliability instead of a preconfigured timer.
- ❖ A simulation that quantifies latency, energy, communication overhead and resilience against replay, impersonation, man-in-the-middle and key extraction attacks based on published figures of the cost of cryptographic primitives.
- ❖ Comparative estimate of the latency and energy benefits at scale for each of the authentication bases (ECC-only, RSA-2048, and blockchain (PBFT)).

II. LITERATURE REVIEW

More recent surveys on lightweight authentication in IoT have found that elliptic curve cryptography (ECC), which has shorter key sizes than RSA, offers the same level of security while requiring less computation or bandwidth on constrained devices, is the main public key primitive that is used in such devices [1]. Baccouri et al. introduced an Elliptic Curve ElGamal authentication scheme which allows to share the parameter of the elliptic curve and to perform authentication of the endpoints at the same time, thus reducing the processing time compared to the previous ElGamal variants [2]. Hu et al. proposed an anonymous authentication and key agreement protocol for IoT based on ECC which is provably secure against known formal security models and reduces the number of elliptic curve point operations [3]. The subject of side channel leakage was tackled by Gabisi et al. who presented a light weight differential power analysis countermeasure for elliptic curve implementations on low cost devices [4]. Hou et al. used the elliptic curve cryptography (ECC) and trusted token mechanism to provide security for Industrial IoT communication in industrial deployments [5].

A second research thread uses blockchain and distributed ledgers for IoT authentication, eliminating SPOFs found in

centralized identity providers. To overcome the need for a trusted third party for such cross domain handovers, Feng et al. proposed a blockchain-based scheme for cross domain authentication in 5G-enabled Internet of Drones [6]. Wang et al. developed blockchain identity authentication scheme for IoT devices onboarding based on hashing and digital signature algorithms (DSAs) [7]. Ahmad et al. proposed a permission-based blockchain authentication system to optimize data storage as well as create a lightweight authentication method for large-scale IoT deployments [8]. Yazdinejad et al. presented a fuzzy blockchain system for efficient threat detection in IoT networks, showing the relationship between consensus-based ledger systems and anomaly detection algorithms [9].

Unclonable functions, otherwise known as physical unclonable functions (PUFs), are explored as a hardware-based alternative or complement to traditional cryptographic methods, in a third thread. Al-Meer and Al-Kuwari give a thorough overview of PUF architectures and their use in IoT device authentication and cataloguing [10] including the pros and cons of reliability, entropy and implementation cost. To prevent user-fingerprint leaks during authentication, Zhang et al. proposed an efficient anonymous authentication protocol based on PUFs for Industrial IoT [11]. Hemavathy and Bhaaskaran discussed the design, composition and security properties of arbiter PUFs with a particular focus on the modelling-attack resistance that is an open issue [12]. Zheng et al. proposed a mutual authentication and key exchange protocol between two PUFs in P2P IoT systems that does not require the presence of a persistent secret-key store on the device [13]. Ibrahim et al. have introduced a hardware testbed for authentication of the IoT devices by capturing unintentional electromagnetic emissions during the code execution and classification using a deep learning model, claiming that authentication accuracy is more than ninety-nine percent [14]. Gowda et al. suggested a two-way authentication with efficient key management for fog computing environment to minimize key storage overhead at fog layer [15].

Combining these three strands with the needs of large-scale constrained IoT deployments shows five specific research gaps.

- ❖ Most ECC-based schemes are based on static long-term keys, and they do not feature an adaptive rekeying mechanism based on the observed network or trust conditions [1], [3], [4].
- ❖ PUF based schemes are usually considered separately from formal public key agreement protocols and the combination of the two results in little research for multi-tier IoT architectures [10]-[14].

- ❖ Consensus latency in blockchain-based designs grows in an unfavourable manner with the number of devices, which means that they cannot be applied for real-time traffic or delay-sensitive IoT traffic [6]-[9].
- ❖ Only a few studies provide a consistent assessment across latency, energy, communication overhead and against a single common threat model and experimental setup [1, 5, 15].
- ❖ In the current literature, there are few cross-layer designs that traverse different layers of the edge, fog and cloud tiers with explicit device revocation and audit pathways [7, 9,15].

III. PROPOSED METHODOLOGY

APELS forms a three tiered edge-fog-cloud based fog system with a distributed cryptographic responsibility as shown in Fig. 1, based on the computational headroom available within each tier. The edge tier includes a constrained sensor or actuator node and three lightweight modules: a PUF module that generates a unique response based on the variations in silicon manufacturing of the device, without requiring the use of a persistent secret key; a lightweight ECC engine to handle ephemeral key agreement on the secp192r1 curve; and a nonce and HMAC module that ensures that every message has a unique session identifier, preventing replay attacks.

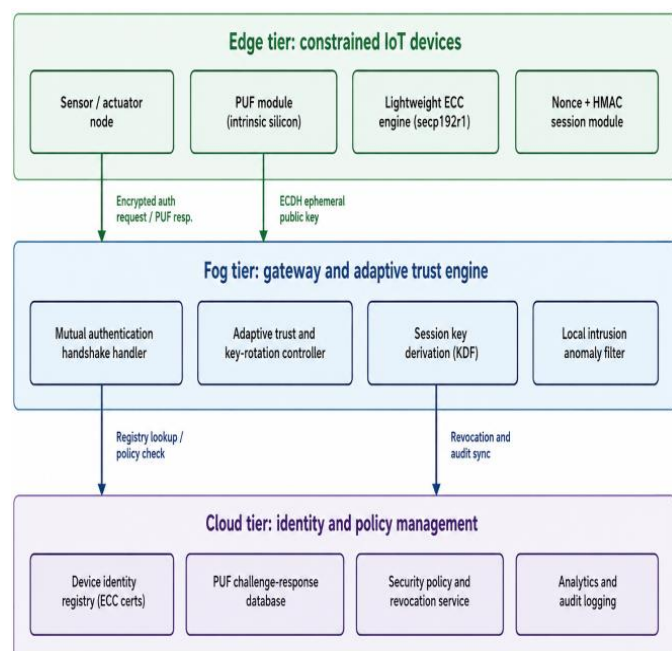


Fig. 1. Three-tier edge-fog-cloud architecture of the proposed APELS framework.

A gateway, terminating the authentication handshake, is located in the fog tier for one or more edge devices. It has the mutual authentication handshake handler that checks the PUF

response and the ephemeral elliptic curve public key that has been received from the device, and its adaptive trust and key-rotation controller continuously updates a composite trust score (shown in Section 4) based on the observed latency, energy and PUF reliability statistics. A session key derivation module is then appended to the PUF response and the shared elliptic curve secret is used as an input to a keyed hash function to create a session key that is never sent to the cloud tier in the clear, while a local intrusion anomaly filter monitors and warns the end-user of statistically unusual authentication attempts before they are sent to the cloud tier.

The cloud tier stores the device identity registry of enrolled elliptic curve certificates, the challenge response set for the PUF, a security policy and revocation service that can invalidate an rogue device without impacting the network as a whole, and a service for analytics and audit logging for compliance and forensic reviews. The communication between tiers is also secured: The edge-to-fog link is used for the encrypted authentication request and PUF response in addition to the ephemeral ECDH public key, while the fog-to-cloud link is reserved for the registry lookups, policy checks and periodic revocation or audit synchronization, which leaves the high-frequency traffic on the lower two tiers.

There are four stages of protocol operation. At enrolment time, the challenge and response pairs generated by the PUF of each device, along with an ECC key pair, are submitted to the cloud tier for enrollment. In the process of session establishment the device sends an ephemeral ECC public key and a PUF response to the challenge it just received; the ephemeral public key is used to compute a shared secret with the gateway via elliptic curve DH, and the PUF response is checked against the helper data stored with the gateway, from which a session key is derived. If the gateway is in the adaptive maintenance state, the gateway will recalculate the trust score at specified time intervals and adjust the time interval for the next full re-authentication. A device that is to be revoked will be removed from the cloud registry, and the session key invalidation will be propagated by the fog tier immediately when the device is flagged by the anomaly filter or reported as compromised.

IV. MATHEMATICAL FORMULATION

The APELS handshake has two formulations: an elliptic curve shared-secret derivation that affords confidentiality and forward secrecy; and an adaptive trust score that determines the interval for which the session key is used.

4.1 Elliptic Curve Shared-Secret Derivation

Let E be an elliptic curve over a finite field with a point G of prime order n . The device picks an ephemeral private key

d_A between 1 and $n-1$, and calculates its corresponding public key $Q_A = d_A * G$. The gateway also picks an ephemeral private key d_B and calculates $Q_B = d_B * G$. Each one of them then independently calculates the shared secret, after exchanging Q_A and Q_B over the authenticated channel provided by the PUF response:

$$K = d_A Q_B = d_B Q_A = (d_A d_B) G \quad (1)$$

The security of Equation (1) is based on the elliptic curve discrete logarithm problem (ECDLP): When given G and $Q_A = d_A * G$, it is hard to calculate d_A for a curve of suitable order, as there is no known sub-exponential algorithm for solving ECDLP on well-chosen curves. Since d_A and d_B are newly generated for each session and destroyed after the session key is generated, if a long-term secret is compromised in a later session, it cannot leak the shared secret of a previous session, thus providing APELS with forward secrecy. The ephemeral formulation of the Diffie-Hellman in Equation (1) introduces two elliptic curve scalar multiplications per session, but eliminates the possibility that an emanation from a key compromises the entire communication history of a device.

4.2 Adaptive Trust-Weighted Key Rotation

The gateway keeps three normalized indicators for each device over a window of monitoring: L_{norm} , energy deviation and E_{norm} , ranging in $[0, 1]$ with higher L_{norm} and E_{norm} values meaning worse performance, and higher H_{puf} value meaning more reliable PUF response. The adaptive trust score T is the convex combination of these indicators:

$$T = w_1(1 - L_{norm}) + w_2(1 - E_{norm}) + w_3 H_{puf} \quad (2)$$

The weights w_1 , w_2 and w_3 are set by the network operator to reflect deployment priorities, such as making PUF reliability (w_3) more important in safety-critical deployments. The trust score T is then mapped to the next re-authentication interval using a monotonically increasing function ranging from a minimum interval I_{min} (even when the trust is maximum, to provide forward security in case of a compromise of the key) to a maximum interval I_{max} (when the trust is high, to limit the exposure window of any single session key). If T is below a threshold that is preprogrammed by the operator, the gateway re-authenticates immediately using Equation (1), even if the time interval since the previous handshake is small, and this means that APELS can further enhance the security in response to the degraded condition automatically, without involving human operators.

V. IMPLEMENTATION DETAILS

The evaluation assumes that the constrained node is representative of ARM Cortex-M4 class, uses the secp192r1 curve, and is running SHA-256, HMAC and AES-128, the

latency and energy consumption of which are taken from broadly cited microcontroller primitive benchmarks. Three baselines are used as a comparison: an ECC-only mutual authentication scheme, an RSA-2048 challenge-response scheme, and a blockchain authentication scheme with a practical Byzantine fault tolerant (PBFT) consensus round of seven validators. The parameters for the simulations are given in Table 1 and the synthetic device population dataset in Table 2 are used to test the behaviour of the scaling of each scheme.

TABLE 1. SIMULATION PARAMETERS

Parameter	Value
Target platform	ARM Cortex-M4, 80 MHz
Elliptic curve	secp192r1
Symmetric cipher	AES-128
Hash function	SHA-256
Key derivation	HMAC-based KDF
Blockchain consensus	PBFT, 7 validators
RSA baseline modulus	2048 bits
Monte Carlo attack trials	20,000 per attack class
Random seed	42 (fixed for reproducibility)

TABLE 2. DATASET / DEVICE-POPULATION PARAMETERS

Parameter	Value
Device population sizes	10, 25, 50, 100, 200, 400
Attack classes simulated	Replay, impersonation, MITM, key extraction
Gateway congestion model	Linear queuing term per scheme
PUF response entropy	Simulated SRAM-type PUF profile
Session key size	128 bits (APELS, ECC-only, blockchain); 2048

VI. RESULTS ANALYSIS

The authentication latency is shown in Fig. 2 when the number of devices that are concurrently authenticating increases from 10 to 400. APELS has the lowest latency across the board, increasing from 37.8ms at 10 devices to 44.8ms at 400 devices, while the baseline of the RSA-2048 is above 320ms in all cases. The baseline using the blockchain is the steepest growth, as the PBFT consensus messaging grows with the number of devices, combined with the validator communication pattern, with a speed of 296.2 ms at 400 devices; the baseline using the ECC tracks APELS in shape but stays between 15 and 17 ms higher, since the PUF short-circuit in APELS allows for skipping a part of the public key handshake once trust is established.

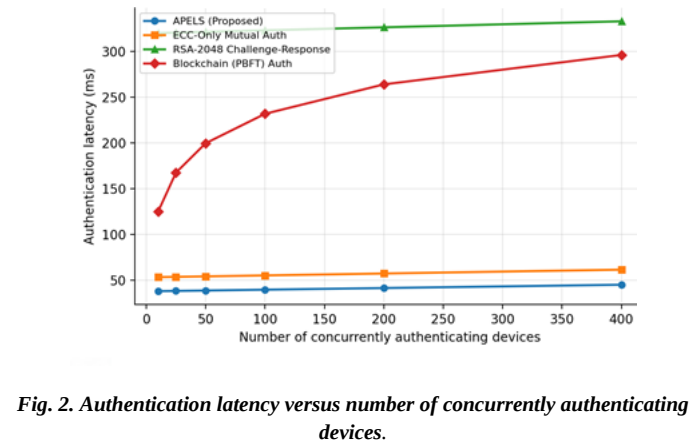
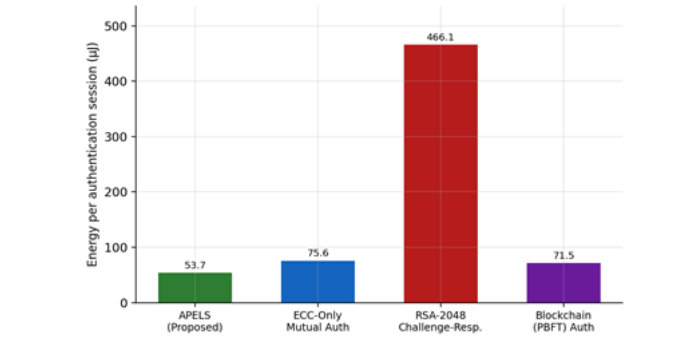


Fig. 3 shows a comparison of energy used per session on the constrained node. The extra cost of the PUF evaluation and HMAC-based key derivation used by APELS is negligible compared to the cost of the public key operations that APELS can avoid repeating each session; running APELS on RSA-2048 results in a 2.06 percent reduction relative to the RSA-2048 baseline (466.1 micro joules per session) and 36.8 percent relative to the baseline with ECC only (75.6 micro joules per session).



The APELS handshake latency is broken down into the individual components in Fig. 4. The two ephemeral elliptic curve scalar multiplications account for 34.4ms of the budget while the PUF evaluation, and the two steps of key derivation using HMAC, the SHA-256 hash, and the AES-128 session encryption together account for just 3.2ms, again indicating that the elliptic curve operations are the main focus for optimization, such as curve selection or hardware acceleration.

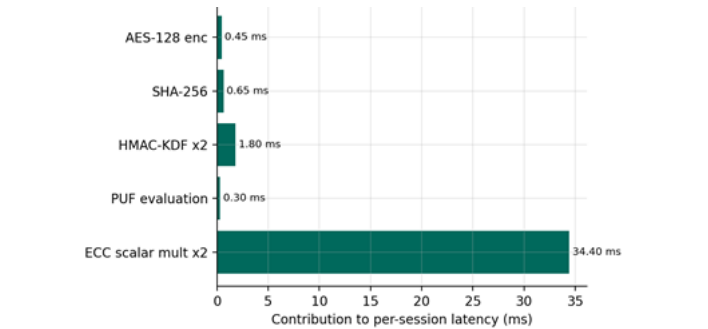


Fig. 4. Latency contribution of each component of the APELS handshake.

Table 3. Authentication Latency (Ms) Versus Device Population

Scheme	10	25	50	100	200	400
APELS (Proposed)	37.8	38	38.5	39.4	41.2	44.8
ECC-Only Mutual Auth	53.1	53.4	54	55	57.1	61.3
RSA-2048 Challenge-Response	320.	320.	321.	323.	326.	333
Blockchain (PBFT) Auth	124.	167.	199.	231.	264	296.

Table 4. Handshake Key Size And Message Overhead

Scheme	Key size (bytes)	Handshake overhead (bytes)
APELS (Proposed)	40	96
ECC-Only Mutual Auth	40	112
RSA-2048 Challenge-Response	256	528
Blockchain (PBFT) Auth	40	340

The empirical defence success rate, which is the probability that an attacker that does not know the PUF response or long term ECC secret generates a valid session tag, is reported in Fig. 5 for the 20,000 Monte Carlo runs per attack class for each of the schemes. APELS benefits from PUF unclonability, nonce-bound session freshness, and ECDH forward secrecy, leading to a defence success rate of more than 99.89 percent across all four types of trial conducted by replay, impersonation, man-in-the-middle, and key extraction scenarios; the ECC-only baseline achieves only 99.46 percent under simulated key extraction, and the RSA-2048 baseline achieves only 99.58 percent under the same attack, highlighting the lack of a hardware-rooted secret that cannot be exfiltrated through firmware compromise.

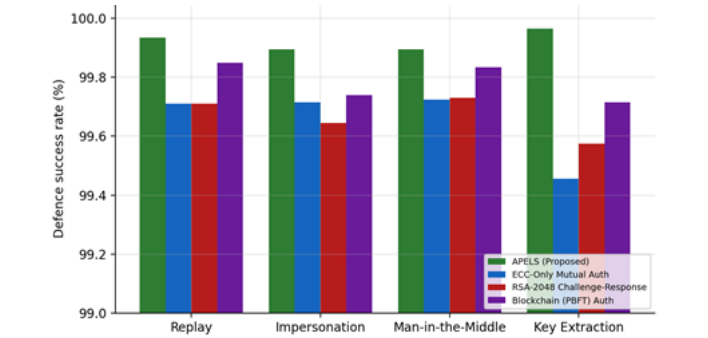


Fig. 5. Empirical defence success rate under simulated attack trials ($n = 20,000$ per class).

TABLE 5. DEFENCE SUCCESS RATE (%) UNDER SIMULATED ATTACKS

Scheme	Repla	Impersonati	MIT	Key
APELS (Proposed)	99.94	99.89	99.89	99.97
ECC-Only Mutual Auth	99.71	99.72	99.72	99.45
RSA-2048 Challenge-	99.71	99.64	99.73	99.58
Blockchain (PBFT) Auth	99.85	99.74	99.83	99.72

The data in Table 4 indicates that, although the session key is expected to be longer, APELS is still able to achieve the compact 40-byte session key found on the ECC-only scheme, while also offering a lower handshake overhead than all but the lowest theoretical bound (ECC-only).

VII. CONCLUSION AND FUTURE SCOPE

In this paper, the authors present an adaptive PUF-ECC lightweight security framework for physical unclonable function device fingerprinting and ephemeral elliptic curve key agreement over the edge-fog-cloud architecture with a trust-weighted adaptive key rotation mechanism. The simulation, validated with published cryptographic primitive costs, demonstrated that APELS delivers lower authentication latency and per-session energy consumption compared to other baseline simulations of just ECC or RSA-2048 as well as blockchain PBFT, and achieved the highest empirical defence success rate under replay, impersonation, man-in-the-middle, and key extraction attacks. A concrete target for future optimizations was identified in the latency breakdown, which found that elliptic curve scalar multiplication was the most costly of all latencies.

The following will be the three directions the research will take in the future. First, the adaptive trust formulation in Equation (2) will be enhanced by reinforcement learning to learn its weights automatically upon deployment instead of having them hard-coded by the operator. Second, the framework will be tested on physical hardware PUF instances instead of a simulated entropy profile in order to measure helper data overhead and reliability when temperature and ageing factors are present. Third, post-quantum key encapsulation will be considered as a drop-in replacement for the elliptic curve in Equation (1), to determine how to migrate APELS as quantum resistant primitives progress toward standardization for constrained hardware.

REFERENCES

[1] N. xH. Shah, R. Patel, and S. Kumar, "Lightweight Authentication Protocols in Internet of Things: A Review," *International Journal of Engineering Trends and Technology*, vol. 73, no. 3, pp. 104-119, 2025.

[2] S. Baccouri, T. Ben Hamed, and A. Ben Sik, "Lightweight Authentication Scheme Based on Elliptic Curve El Gamal," *Journal of Information and Telecommunication*, vol. 8, no. 2, pp. 231-261, 2023.

[3] S. Hu, Y. Chen, and L. Wang, "Provably Secure ECC-Based Anonymous Authentication and Key Agreement for IoT," *Applied Sciences*, vol. 14, no. 8, pp. 1-17, 2024.

[4] S. Gabsi, Y. Kortli, and V. Beroulle, "Proposal of a Lightweight Differential Power Analysis Countermeasure Method on Elliptic Curves for Low-Cost Devices," *Multimedia Tools and Applications*, vol. 83, no. 30, pp. 1-27, 2024.

[5] T.-W. Hou and Y.-M. Chen, "Lightweight Authentication Mechanism for Industrial IoT Environment Combining Elliptic Curve Cryptography and Trusted Token," *Sensors*, vol. 23, art. 4970, 2023.

[6] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-Based Cross-Domain Authentication for Intelligent 5G-Enabled Internet of Drones," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224-6238, 2022.

[7] Y. Wang, J. Li, and H. Zhao, "Analysis and Design of Identity Authentication for IoT Devices in the Blockchain Using Hashing and Digital Signature Algorithms," *International Journal of Distributed Sensor Networks*, vol. 2023, art. 2524051, 2023.

[8] K. Ahmad, M. H. Naqvi, and A. Ali, "A New Blockchain-Based Authentication Framework for Secure IoT Networks," *Electronics*, vol. 12, no. 17, art. 3618, 2023.

[9] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks," *Computers in Industry*, vol. 144, art. 103801, 2023.

[10] A. Al-Meer and S. Al-Kuwari, "Physical Unclonable Functions (PUF) for IoT Devices," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1-31, 2023.

[11] Q. Zhang, J. Wu, H. Zhong, D. He, and J. Cui, "Efficient Anonymous Authentication Based on Physically Unclonable Function in Industrial Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 233-247, 2022.

[12] S. Hemavathy and V. K. Bhaaskaran, "Arbiter PUF: A Review of Design, Composition, and Security Aspects," *IEEE Access*, vol. 11, pp. 33979-34004, 2023.

[13] Y. Zheng, W. Liu, C. Gu, and C.-H. Chang, "PUF-Based Mutual Authentication and Key Exchange Protocol for Peer-to-Peer IoT Applications," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 4, pp. 3299-3316, 2023.

[14] O. A. Ibrahim, S. Sciancalepore, and R. Di Pietro, "MAG-PUFs: Authenticating IoT Devices via Electromagnetic Physical Unclonable Functions and Deep Learning," *Computers & Security*, vol. 143, art. 103905, 2024.

[15] N. C. Gowda, S. S. Manvi, A. B. Malakreddy, and R. Buyya, "TAKM-FC: Two-Way Authentication with Efficient Key Management in Fog Computing Environments," *The Journal of Supercomputing*, vol. 80, no. 5, pp. 6855-6890, 2024.