International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 15 Issue 2 pp. 9-18 June - Dec 2023 www.csjournals.com

Lightweight Cryptographic Techniques for Secure Data Transmission in IoT

Priyanka Jangra
Department of Electronics & Communication Engineering, University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, INDIA

Abstract: Efficient mechanisms for secure data transmission are required in the Internet of Things (IoT) where devices have limited resources. Some conventional cryptographic algorithms may impose too much computing, memory, energy and communications overhead on these types of devices. This paper reviews lightweight cryptographic techniques for securing IoT data transmission such as lightweight symmetric and stream ciphers, lightweight hash/MAC functions, lightweight authenticated encryption, ECC based schemes and authentication/key exchange protocols. These techniques are contrasted in terms of security, throughput, energy consumption, hardware area and implementation suitability. The analysis reveals that lightweight primitives can offer a good compromise between security and resource efficiencies, and hybrid designs that integrate lightweight Symmetric Encryption and ECC based Key Establishment are especially suitable for constrained IoT environments. The results give a brief base to the selection of lightweight cryptographic mechanisms for secure and efficient IoT data transmission.

Keywords: Internet of Things; lightweight cryptography; block ciphers; elliptic curve cryptography; secure data transmission; resource-constrained devices; IoT security.

1. Introduction

Connected IoT endpoints have become not only a niche research interest but also an implemented infrastructure in areas like smart metering, precision agriculture, industrial control, connected healthcare and smart-city sensing. The majority of these endpoints are extremely limited: they are based on 8- or 16-bit microcontrollers, have few kilobytes of RAM, and are powered by coin-cell batteries or energy harvesting instead of mains power. Perception-level data is frequently sent via multi-hop, low-power wireless networks, to a gateway and, ultimately, to the cloud. All hops are places where confidentiality, integrity, and authenticity may be attacked by eavesdropping, node capture, replay or man-in-the-middle attacks. Traditional cryptographic primitives AES with big block schedules, RSA with multi-kilobit moduli, and hash functions in the SHA-2 family are designed to be run on servers and desktops, and their direct implementation on small nodes results in unacceptable latency, power consumption and software size. The problem of secure data transmission in this context is not an algorithm selection, but a layer of decisions: which symmetric cipher should be used to guarantee payload confidentiality, which hash or MAC should be used to guarantee integrity, how the keys are created and swapped between devices with no display or keyboard, and how these decisions interact with duty-cycled radios and lossy links. There is extensive and scattered literature that suggests different individual ciphers, hash functions and protocols, optimised to different points of the design space (area, latency, energy, or code size). This fragmentation encourages a consolidated overview with a specific emphasis on the security of data-transmission, but not on lightweight cryptography overall.

In this paper, four main contributions are made: the review of major lightweight cryptographic techniques for secure IoT data transmission, including symmetric ciphers, stream ciphers, hash/MAC functions, AEAD, ECC, and authentication and key-exchange protocols; comparison of the representative techniques based on security, throughput, energy usage, hardware area and suitability for resource-constrained devices; examination of the key security requirements addressed by these techniques such as confidentiality, integrity, authentication and freshness; and the identification of major research challenges including side-channel resistance, scalable key management, cross-layer security, post-quantum readiness, and reduced-round cryptanalysis. The rest of the paper is organized as follows: In Section 2, the IoT security landscape and threat model are presented. In Section 3, the fundamentals and taxonomy of lightweight cryptography are discussed. In Section 4, major lightweight cryptographic techniques are reviewed. In Section 5, open challenges and future research directions are discussed and presented, and finally, Section 6 concludes the paper.

2. IoT Security Landscape and Threat Model

The first step towards understanding why standard cryptography under-performs on IoT nodes is to characterize the constraints imposed on the device, and map those constraints on a layered architecture and associated attack surface.

2.1 Resource Constraints of IoT Devices

The IETF definition of constrained-node network categorizes the classes of devices according to amount of RAM and ROM/Flash that is available, which are directly related to the amount of cryptographic code or working memory an implementation can use [21]. Class 0 devices (with less than around 10 KiB RAM / 100 KiB Flash) cannot run a full IP stack; nor a general purpose TLS library, and rely on gateway mediated security; Class 1 devices are able to run a constrained protocol stack (e.g., CoAP/DTLS) but not comfortably a full browser grade cipher suite; Class 2 devices are approaching the capability of a low end smartphone and can largely reuse conventional cryptography. This classification is summarised in Table 1, together with typical implications to lightweight-cryptography.

Table 1. IoT device constraint classes and cryptographic implications (after RFC 7228 [21]).

Class	Typical RAM	Typical ROM/Flash	Cryptographic implication
Class 0	< 10 KiB	< 100 KiB	Cannot host general-purpose crypto libraries; relies on lightweight ciphers or gateway-side security
Class 1	~ 10 KiB	~ 100 KiB	Can run a constrained stack (CoAP/DTLS) with compact block ciphers and lightweight hash functions
Class 2	~ 50 KiB	~ 250 KiB	Can approximate conventional crypto (AES, ECC) with careful optimisation
Gateway/Edge	> 1 MiB	> 1 MiB	Can run full TLS/DTLS 1.2+, standard AES-GCM, RSA/ECC key exchange

2.2 Layered Architecture and Attack Surface

One popular abstraction is to split the IoT protocol stack into three layers: Perception (perception) layer (sensors, RFID tags, actuators); Network (connectivity) layer (short-range protocols, low-power wide-area protocols such as 6LoWPAN, Zigbee, BLE and LoRaWAN, which transport the application data via MQTT or CoAP); and Application (action) layer (cloud/edge services and control logic). This architecture (and the most important threat at each layer) is shown in Figure 1.

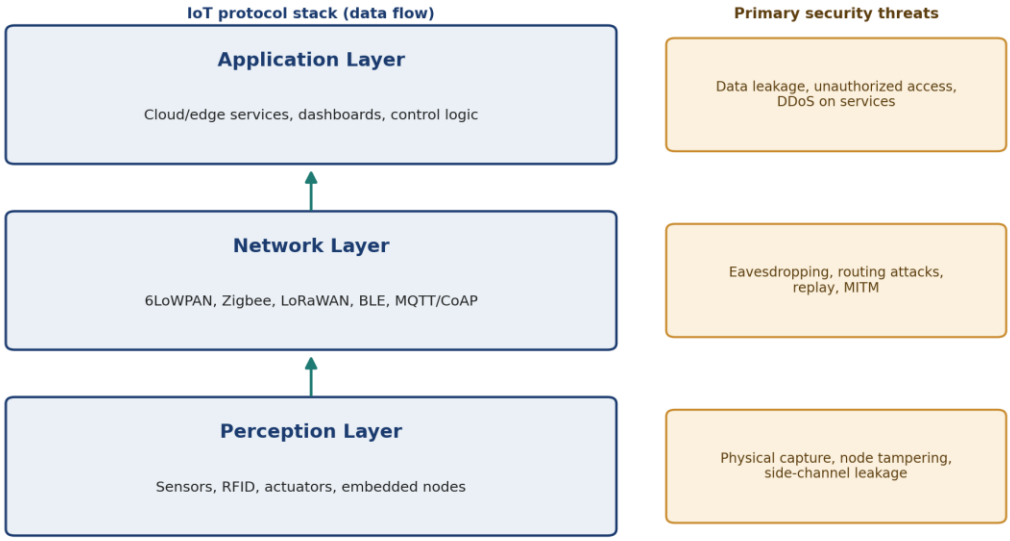

Fig. 1. Three-layer IoT architecture with the dominant class of security threat at each layer.

The perception layer includes physical access to a device that can result in node capture, tampering, and power and/or timing analysis to obtain cryptographic keys directly from the hardware [11]. In the network layer, the broadcast nature of wireless links makes the traffic vulnerable to eavesdropping, selective forwarding, sinkhole and replay attacks, especially if not designed for authentication [13]. From the application layer, aggregated data in the cloud or the edge tier is a valuable target for abuse and denial of service attacks targeting dashboards and control APIs [14]. Secure data transmission must be thought of as end-to-end and a characteristic of no single hop, since if one hop is compromised then it is possible to break the security guarantees offered by other hops.

2.3 Security Requirements for Data Transmission

Confidentiality, which means that payload data is not readable by an eavesdropper monitoring the wireless medium; integrity, which means that data in transit cannot be altered; authenticity, which means that a receiver can verify the origin of a message (usually with either a lightweight MAC or digital signature); and freshness, which means that recorded traffic cannot be replayed successfully. [12], [19].

3. Fundamentals and Taxonomy of Lightweight Cryptography

3.1 Design Goals and Evaluation Metrics

Lightweight cryptography is not an easing of security requirements, it’s a re-optimisation of the cost model. Unlike conventional cryptographic design for which the primary criteria is the throughput

achievable on a server-class CPU, lightweight design considers throughput, hardware area (in Gate Equivalents, GE for ASIC/FPGA implementations), RAM/ROM footprint (for software implementations on microcontrollers), energy per encrypted bit, and latency, and aims to optimise for these metrics while maintaining resistance to differential, linear, algebraic and side-channel cryptanalysis [11] [20] [1]. This trade-off space was formalised in the NIST Report on Lightweight Cryptography [20] which catalogued the various lightweight candidate primitives considered along these metrics and presented its conclusions to the NIST Lightweight Cryptography standardisation process. One common theme in the literature surveyed is that no single primitive is dominant when it comes to each of these metrics in isolation: bit-sliced ARX ciphers generally have the highest software throughput, S-box based ciphers generally have the smallest hardware footprint, and general purpose block ciphers like AES are generally competitive in security margin at the price of footprint [1, 2, 11].

3.2 Taxonomy of Lightweight Cryptographic Primitives

The primitives surveyed in this review are grouped in four families: symmetric-key (block and stream) primitives, asymmetric-key (public-key) primitives, hash/MAC functions and authentication and key exchange protocols, which usually make up the previous three families into an end-to-end secure-transmission scheme shown in fig 2.

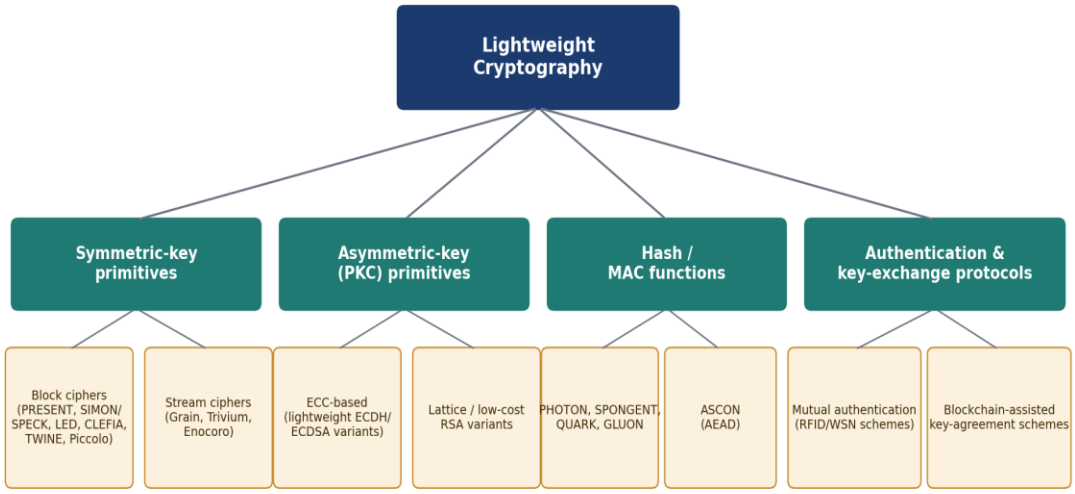

Fig. 2. Taxonomy of lightweight cryptographic techniques surveyed in this review.

In the lightweight-cryptography literature, symmetric-key primitives are predominant because symmetric operations (substitution-permutation networks or ARX structures) are easy to map onto constrained hardware or software. Public-key primitives are relatively costly but have to be used where key distribution needs to be scalable; elliptic curve cryptography (ECC) is the de facto lightweight alternative to RSA with a comparable security level at significantly smaller key sizes [9] [10]. Integrity and message authentication can be achieved by using Hash and MAC functions – these were designed for hardware-constrained environments in PHOTON and SPONGENT [3]. Above these primitives, authentication and key-exchange protocols are most of the attention in the IoT literature and are application-specific.

4. Lightweight Cryptographic Techniques for Secure IoT Data Transmission

4.1 Lightweight Symmetric Block Ciphers

Block ciphers continue to be the workhorse for bulk payload confidentiality when transmitting IoT data. The PRESENT 64-bit substitution-permutation network was developed in the early stages of the development of ciphers designed for extreme hardware compactness, with a 4-bit S-box that requires about 1,570 GE [1]. The SIMON and SPECK families, initiated by the NSA, provide parameterised block and key sizes, and represent two different designs: an S-box free ARX design (SPECK, software oriented) and a small Feistel like design (SIMON, hardware oriented) [2]. LED is an AES-like structure with an S-box derived from PRESENT with the minimum area overhead in key scheduling [4]. Standardized by ISO/IEC 29192, CLEFIA is a four-branch generalized Feistel network that provides a good security-to-footprint ratio for moderately capable devices [5]. TWINE aims for a compromise between software and hardware optimization with a Type-2 generalised Feistel structure [6] and reduced-round TWINE is shown to be vulnerable to related-key impossible-differential attacks, as for any lightweight ciphers, this indicates the need for active cryptanalytic research [17]. The design parameters of these ciphers and the AES-128 basic line are summarised in Table 2.

Table 2. Representative lightweight block ciphers for IoT data confidentiality.

Cipher	Year	Structure	Block / Key (bits)	Rounds	Primary target
PRESENT	2007	SPN	64 / 80,128	31	Hardware (ASIC/RFID) [1]
SIMON	2015	Feistel (ARX-free)	32–128 / up to 256	32–72	Hardware-optimised [2]
SPECK	2015	ARX	32–128 / up to 256	22–34	Software-optimised [2]
LED	2011	AES-like SPN	64 / 64,128	32,48	Hardware, minimal key schedule [4]
CLEFIA	2007	4-branch GFN	128 / 128,192,256	18–26	Balanced HW/SW [5]
TWINE	2012	Type-2 GFN	64 / 80,128	36	Balanced HW/SW [6]
Piccolo	2011	Feistel	64 / 80,128	25,31	RFID / sensor nodes [7]
AES-128 (baseline)	2001	SPN	128 / 128	10	General purpose

4.2 Lightweight Stream Ciphers

Grain, Trivium and Enocoro are stream ciphers with very low gate counts, which were shortlisted in the eSTREAM hardware profile for their suitability for continuous sensor telemetry which avoids the padding overhead of block ciphers.[16], [19].

4.3 Lightweight Hash Functions and Message Authentication

Many authentication protocols rely on hash functions, which are also used for integrity checking. The PHOTON construction of the sponge is done with an internal permutation similar to that of AES, to reduce the size of the state, aiming at hardware of the size of RFID tags [3]. SPONGENT and QUARK follow the same sponge philosophy, but have different permutation design to give a choice between digest size and gate count. More recently the ASCON family has been chosen by NIST as the primary Lightweight Cryptography standard for authenticated encryption with

associated data (AEAD) both of which provide confidentiality and integrity in one primitive, a permutation [8].

Table 3. Lightweight hash / authenticated-encryption primitives for integrity protection.

Primitive	Year	Construction	Digest / tag size	Notes
PHOTON	2011	AES-like sponge	80–256 bits	Compact hardware hashing for RFID [3]
SPONGENT	2011	Sponge (PRESENT-like)	88–256 bits	Very low gate count variants
QUARK	2010	Sponge	136–256 bits	eSTREAM-inspired permutation
ASCON	2016/2021	Sponge, AEAD	128-bit tag	NIST LWC standard; combines enc. + auth. [8]

4.4 Lightweight Public-Key and ECC-Based Schemes

The direct result of using elliptic curve cryptography is a reduction in the number of bits in the public key, which translates into a reduction in transmission overhead, storage and cost of point-multiplication on constrained CPUs [9,10]. The choice of curves is often combined with lightweight elliptic-curve Diffie–Hellman (ECDH) for session-key agreement and ECDSA or its lightweight variants for signing with further implementation-level optimisations (fixed-base comb multiplication, projective coordinates) to achieve even fewer cycles on 8/16-bit MCUs [12] and [13]. Table 4 gives a comparison between ECC and RSA, at the same security levels.

Table 4. ECC versus RSA key sizes at matched security levels (NIST-equivalent) [9], [10], [20].

Security level (bits)	RSA modulus	ECC key size	Approx. size reduction
80	1024 bits	160 bits	~6.4×
112	2048 bits	224 bits	~9.1×
128	3072 bits	256 bits	~12×
192	7680 bits	384 bits	~20×

4.5 Lightweight Authentication and Key-Exchange Protocols

The primitives described above must be combined into authentication and key-management protocols that are end-to-end secure and appropriate for the use of devices lacking displays and keyboards. Mutual-authentication schemes for RFID or WSN usually involve a lightweight hash function or block cipher, in addition to a challenge-response mechanism to tie a session key to a verified device identity [15], [16]. In more recent proposals, consortium blockchains are used to implement a decentralised and cross-domain authentication that dispenses with a single trusted key-distribution centre, albeit at the cost of increased communication overhead and the elimination of the central authority [22]. At the survey level, the literature surveyed [12] and [23] also shows the hybrid scheme using a lightweight block cipher for bulk data and an ECC based handshake for session-key establishment to be the most prevalent.

Table 5. Categories of lightweight authentication and key-exchange protocols for IoT.

Category	Representative approach	Primitives used	Typical target
Challenge-response mutual auth.	Hash/MAC-based handshake	Lightweight hash, symmetric cipher	RFID tags, WSN nodes [15]
ECC-based key agreement	ECDH session-key establishment	ECC, lightweight block cipher	Gateway–device sessions [12]
Blockchain-assisted authentication	Consortium blockchain identity binding	Hash, digital signature, consensus	Cross-domain IoT [22]
Group / broadcast authentication	Shared group key with periodic rotation	Symmetric cipher, lightweight MAC	Smart metering, sensor fleets [23]

Table 6. Aggregated indicative performance metrics for the compared ciphers.

Cipher	Throughput (kbps)	Energy (µJ/bit)	Hardware area (GE)
PRESENT-80	200	1.9	1,570
SIMON-128	950	1.1	763
SPECK-128	1,100	0.9	693
LED-64	100	2.6	966
CLEFIA-128	620	1.4	2,488
TWINE-80	430	1.7	1,503
Piccolo-80	240	2.1	1,136
AES-128 (baseline)	1,450	3.0	3,100

Table 7. Summary of key surveyed works on lightweight cryptography for IoT.

Author(s), Year	Focus	Key contribution
Hatzivasilis et al., 2018 [11]	Block cipher review	Structured review of 60+ lightweight block ciphers with design-goal classification
Dhanda et al., 2020 [12]	LWC for IoT security	Maps lightweight primitives to IoT security requirements and constraints
Khan et al., 2021 [13]	Constrained-device protocols	Survey of lightweight cryptographic protocols for constrained IoT devices
Rana, Mamun & Islam, 2022 [14]	LWC in IoT networks	Comparative analysis of contemporary symmetric/asymmetric ciphers for IoT
Okello et al., 2017 [16]	Early LWC survey	State-of-the-art snapshot of lightweight cryptography for IoT circa 2017
Gunathilake et al., 2019 [19]	Next-gen LWC	Implementation challenges for next-generation lightweight cryptography
Zhang et al., 2022 [22]	Blockchain authentication	Consortium-blockchain-based lightweight cross-domain IoT authentication

5. Open Challenges and Future Research Directions

Although significant advances have been made, there are open problems in the surveyed literature that hinder the transition to deployed, standardised practice.

Table 8. Open challenges identified across the surveyed literature.

Challenge	Description	Representative sources
Standardisation gap	Multiple competing lightweight ciphers with no single dominant standard until NIST's LWC process matured	[1], [18], [20]
Side-channel resistance	Compact implementations often sacrifice masking/countermeasures that protect against power/timing analysis	[11], [15]
Key management at scale	Distributing and rotating keys across thousands of constrained, intermittently connected nodes remains costly	[12], [22]
Post-quantum readiness	Lightweight ECC schemes are vulnerable to large-scale quantum attacks; lightweight post-quantum primitives are immature	[9], [10], [20]
Cross-layer security	Cryptographic protection at one layer does not compensate for weaknesses at another (e.g., routing-layer attacks)	[13], [14]
Cryptanalysis of reduced-round variants	Some lightweight ciphers show weaknesses in reduced-round or related-key settings, requiring conservative parameterisation	[17]

NIST's Lightweight Cryptography project, working on the standardisation gap, whittled down a large group of candidates to ASCON as the leading AEAD standard, to which future implementation and side-channel-hardening effort will probably be focused [8], [20]. Side-channel resistance is still an open engineering problem as it generally leads to the re-introduction of overheads in area and latency that lightweight design aims to avoid, raising engineering tensions between these two objectives [11]. Scalable key management is perhaps the least solved problem in the literature surveyed: most of the proposed protocols are tested in small testbeds and the behaviour of these protocols under churn, node failure and large-scale rekeying has yet to be well characterised [12], [22]. The need for post-quantum migration is an emerging, but not a mature, issue in the surveyed publications as most of the schemes surveyed predate the advent of lightweight post-quantum candidates; however, it is consistently mentioned as a medium-term risk because of the long service life of deployed IoT hardware [20]. Lastly, the cryptanalytic results on reduced-round variants of ciphers like TWINE show that lightweight primitives can be as much of a target as traditional ciphers and that parameter values (e.g. number of rounds) should not be minimized for efficiency reasons, but kept with a large security margin.

6. Conclusion

This review focused on lightweight cryptographic schemes with the aim of securing data transmission in resource constrained IoT systems. Lightweight block ciphers, stream ciphers, hash/MAC functions, authenticated encryption, ECC-based schemes and authentication/key exchange mechanisms were analysed. The comparison gives an idea of how much more the computational, energy, memory and hardware requirements can be reduced without compromising the important security properties, thereby proving that lightweight cryptography can play a very important role for this purpose. Specifically, texts analysed show that a hybrid scheme of ECC-based key establishment and lightweight symmetric encryption for data protection can be used practically for constrained IoT devices. However, many key issues arise, including side channel protection, scalable key management, cross-layer security, migration towards post-quantum era and security of reduced-round lightweight ciphers. Future research efforts should thus target energy-efficient, scalable, standardized, well-validated lightweight cryptographic solutions enabling end-to-end security in a wide range of IoT applications.

References

[1] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," in Proc. CHES 2007, LNCS vol. 4727, Springer, 2007, pp. 450-466.

[2] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Lightweight Block Ciphers," in Proc. 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015, pp. 1-6.

[3] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON Family of Lightweight Hash Functions," in Proc. CRYPTO 2011, LNCS vol. 6841, Springer, 2011, pp. 222-239.

[4] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED Block Cipher," in Proc. CHES 2011, LNCS vol. 6917, Springer, 2011, pp. 326-341.

[5] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit Blockcipher CLEFIA," in Proc. FSE 2007, LNCS vol. 4593, Springer, 2007, pp. 181-195.

[6] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, "TWINE: A Lightweight Block Cipher for Multiple Platforms," in Proc. SAC 2012, LNCS vol. 7707, Springer, 2012, pp. 339-354.

[7] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "Piccolo: An Ultra-Lightweight Blockcipher," in Proc. CHES 2011, LNCS vol. 6917, Springer, 2011, pp. 342-357.

[8] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," Journal of Cryptology, vol. 34, no. 3, article 33, 2021.

[9] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203-209, 1987.

[10] V. S. Miller, "Use of Elliptic Curves in Cryptography," in Proc. CRYPTO 1985, LNCS vol. 218, Springer, 1986, pp. 417-426.

[11] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A Review of Lightweight Block Ciphers," Journal of Cryptographic Engineering, vol. 8, no. 2, pp. 141-184, 2018.

[12] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," Wireless Personal Communications, vol. 112, pp. 1947-1980, 2020.

[13] M. N. Khan, A. Rao, and S. Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4132-4156, 2021.

[14] M. Rana, Q. Mamun, and M. R. Islam, "Lightweight Cryptography in IoT Networks: A Survey," Future Generation Computer Systems, vol. 129, pp. 77-89, 2022.

[15] I. Bhardwaj, A. Kumar, and M. Bansal, "A Review on Lightweight Cryptography Algorithms for Data Security and Authentication in IoTs," in Proc. Int. Conf. on Signal Processing, Computing and Control (ISPCC), Solan, India, 2017, pp. 504-509.

[16] W. J. Okello, Q. Liu, F. A. Siddiqui, and C. Zhang, "A Survey of the Current State of Lightweight Cryptography for the Internet of Things," in Proc. Int. Conf. on Computer, Information and Telecommunication Systems (CITS), Dalian, China, 2017, pp. 292-296.

[17] Y. Wei, P. Xu, and Y. Rong, "Related-Key Impossible Differential Cryptanalysis on Lightweight Cipher TWINE," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 2, pp. 509-517, 2019.

[18] S. B. Sadkhan and A. O. Salman, "A Survey on Lightweight-Cryptography Status and Future Challenges," in Proc. Int. Conf. on Advance of Sustainable Engineering and its Application (ICASEA), IEEE, 2018, pp. 105-108.

[19] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications," in Proc. IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 707-710.

[20] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Report on Lightweight Cryptography," NIST Internal Report NISTIR 8114, National Institute of Standards and Technology, 2017.

[21] C. Bormann, M. Ersue, and A. Keranen, "Terminology for Constrained-Node Networks," IETF RFC 7228, 2014.

[22] Y. Zhang, Y. Luo, X. Chen, F. Tong, Y. Xu, J. Tao, and G. Cheng, "A Lightweight Authentication Scheme Based on Consortium Blockchain for Cross-Domain IoT," Security and Communication Networks, vol. 2022, article 9686049, 2022.

[23] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced Lightweight Encryption Algorithms for IoT Devices: Survey, Challenges and Solutions," Journal of Ambient Intelligence and Humanized Computing, 2017.